



SPARTA

D12.5

Final report on dissemination and communication and evaluation – v3

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1 st February, 2019
Duration	41 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D12.5 / V1.0
Work package contributing to the deliverable	WP12
Due date	June 2022 – M41
Actual submission date	8 th July, 2022

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

Abstract	The present deliverable contains the final report and evaluation of the work carried out in each stage of the dissemination and communication planned actions in the D12.4 – Updated dissemination and communication plan and evaluation.
Keywords	Communication & dissemination strategy, engagement 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)

Elisabete Carreira (INOV)

Reviewers (ordered according to beneficiary numbers)

Diane Bahrami (CEA)

Martin Zadnik (CESNET)

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 updates and final evaluation of the work carried out in each stage of the communication and dissemination (C&D) plan during the third year of the SPARTA project.

Chapter 1 situates the present deliverable in the scope of the SPARTA activities and describes the collaborative interactions between the WP12 and the other WPs of the project.

Chapter 2 reviews the strategic axes established in the C&D plan, the messages selected to be delivered during the third year of the project and the contribution of the communication and dissemination activities to the overall project's KPIs. It contains a brief summary of the activities developed in the scope of the Cyber Competence Network.

Chapter 3 reports and evaluates the actions developed by the SPARTA partners during the third year of the project to disseminate and communicate project's aims, values, and results. These actions range mainly from participation and organization of events, conferences, and workshops to scientific publications. The actions designed for the third year of the project related to tasks 12.4 *Closing the Gender and Diversity Gap* and 12.5 *Engagement of the Outermost Regions of Europe – “Go Cyber with SPARTA” campaign* are addressed in deliverable 12.6 and 12.7, respectively, and shortly summarized here.

Chapter 4 reviews the Communication and Dissemination instruments efficiency to keep SPARTA audiences engaged with the project and to deliver coherent and dynamic messages.

Chapter 5 provides a general evaluation of the implementation of the plan, the communication and dissemination actions and related instruments.

Chapter 6 summarizes the main lessons learned during the three years of the SPARTA project.

Table of Content

Chapter 1	Introduction	1
Chapter 2	Communication Strategic Approach	2
2.1	Strategic Axes	2
2.2	Key Audiences and Messages	2
2.3	Contribution to the KPIs of the project	3
2.4	Cyber Competence Network	4
Chapter 3	Communication and Dissemination actions	5
3.1	Conferences, workshops and other events	5
3.2	Scientific Publications	29
3.3	Monthly SPARTA workshops	57
3.4	Campaigns for Diversity in Cybersecurity	57
3.4.1	Closing the Gender Gap	57
3.4.2	Outermost Regions Engagement	57
Chapter 4	Communication and Dissemination Instruments	59
4.1	SPARTA Official Website	59
4.2	SPARTA social media	60
4.2.1	LinkedIn	61
4.2.2	Instagram	62
4.2.3	Twitter	63
4.3	Contribution of partner to C&D activities	63
4.4	Media Relations	63
4.5	Podcasts	64
4.6	Videos	65
4.7	Demonstrators	65
4.8	Internal Communication Instruments	65
4.8.1	SPARTA NEWS	65
4.8.2	NextCloud	66
4.9	Review Recommendations	66
Chapter 5	Third-year general evaluation	67
Chapter 6	Summary and Conclusion	68
	List of Abbreviations	70
	Annex 1 – Twitter Analytics	71
	Bibliography	83

List of Figures

Figure 1: CCN at FIC 2021	4
Figure 2: SPARTA Website front page.....	59
Figure 3: 2021 Monthly History of Visitors to the Website	60
Figure 4: 2022 Monthly History of Visitors to the Website	60
Figure 5: LinkedIn visitor metrics 2020-2021	61
Figure 6: LinkedIn visitor metrics 2022.....	61
Figure 7: LinkedIn visitor demographics (top job functions 2020-2022).....	62
Figure 8: LinkedIn visitor demographics (top industries 2022).....	62
Figure 9: Age and gender of SPARTA Audience on Instagram	63

List of Tables

Table 1: SPARTA Messages for M24-M36, Action Axis	3
Table 2: Contribution to the KPIs of objective 6.....	3
Table 3: Contribution to the KPIs of objective 3.....	4
Table 4: Updated and final list of the SPARTA events	29
Table 5: Final List of SPARTA Scientific publications.....	56
Table 6: SPARTA presence on media platforms	64

Chapter 1 Introduction

The WP12 – Communication and Dissemination - is conceived to plan, coordinate, and execute all the activities related to the dissemination and communication of the SPARTA project. It foresees the yearly update of the strategic plan designed within the deliverable 12.1 – *Dissemination and communication plan, updates and evaluation* (hereinafter C&D plan) – jointly with the evaluation of the work carried out during the previous year.

The present deliverable is the final report of the communication and dissemination activities carried out during the third year of the project and provides an evaluation of the updates made in deliverable D12.4.

From an early stage, the WP12 relied on ongoing interactions with the SPARTA WPs to receive inputs that allowed for the correct implementation of the activities planned in the C&D plan, and for the necessary updates to it, both in D12.3 and D12.4.

As established in the previous deliverable D12.4 – *Dissemination and communication plan, updates and evaluation* – interactions with all the partners have been leveraged to ensure strong internal communication and a diverse and complete set of contents to disseminate via SPARTA communication channels, keeping both partners and audiences well informed of SPARTA activities and achievements.

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

The relations with WP3 – Roadmap Design – and WP8 – Clustering, platforms, and ecosystems – have been equally important to achieve the proposed KPIs and to build sustained collaborations with the cybersecurity community, through the organisation and communication (through the SPARTA official website, social media accounts and the internal mailing list) of the monthly SPARTA workshops, and other events.

During the third year, and the extension period conceded to conclude project activities, the WP12 actively interacted with the SPARTA programs (T-SHARK, CAPE, HALL-T, and SAFAIR) to ensure that the project results were duly communicated to the SPARTA community, both internally (partners, associates and friends) and externally (target groups reached through social media, media platforms, the website and events).

Chapter 2 Communication Strategic Approach

This chapter reviews the strategic axes established in the C&D plan, the messages selected to be delivered during the third year of the project and the contribution of the communication and dissemination activities to the overall project's KPIs. A brief summary of the activities developed in the scope of the Cyber Competence Network are addressed in this chapter.

2.1 Strategic Axes

The three interdependent strategic axes established in deliverable 12.1 served as the grounding basis to conduct and develop all the activities done during the project's lifetime:

- **Awareness building:** making the project and its aims acknowledged.
- **Participation:** engaging target groups and enable them to understand SPARTA concepts and achieved results.
- **Action:** promoting action from target groups influencing practices, products and standards.

The first version of the plan defined the **Action** axis as the third-year approach, conceived to target the communication and dissemination efforts at changing attitudinal behaviour, that is of public interest, towards cybersecurity actions such as the 1) adoption of cybersecurity habits; 2) the acquisition from the industries of cybersecurity services; and the 3) academy starting to direct their interests and activities towards the issue.

A third-year general evaluation follows to assess the achievement of the communication objectives proposed for the **Action** axis, as well as for the **Awareness building** and **Participation** axes.

2.2 Key Audiences and Messages

SPARTA key audiences were identified and characterized in deliverable 12.1 as well as the key messages to be delivered during the third year of the project, for the placement of the **Action axis**, highlighted below. The messages were duly delivered through SPARTA social media accounts, website, events and other media platforms. Overall, the identification of messages and key audiences served as the basis to successfully make the project, its aims, values and results known. The length of reach to our targeted audiences will be described in chapter 3 and 4.

Dimension	Messages
Gender equality	Understand and work on the gender and diversity gap issue is a social responsibility of public interest. As to reduce the gender gap and lack of human resources for cybersecurity in Europe, SPARTA will address this issue by embedding several positive actions.
Inclusion and diversity	Contributing to a more inclusive society, SPARTA addresses diversity in its multiple forms by promoting the engagement of associated partners, stakeholders, and end-users, considering geographical, cultural, societal, and sectoral diversity.
SPARTA impact	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 European

Dimension	Messages
	Union to raise awareness and to foster conversations ranging from cutting-edge research advances to accurate problem identification.
SPARTA results	SPARTA’s research roadmap starts from horizontal technologies: major technological drivers like digitization, Big Data, artificial intelligence, cognitive Internet, and IoT, based on cybersecurity assets such as blockchain technology, as well as new trends like programmable materials, or quantum computers, will already have significant impacts on all industrial sectors.

Table 1: SPARTA Messages for M24-M36, Action Axis

2.3 Contribution to the KPIs of the project

The D12.1 had foreseen the direct contributions of the communication and dissemination activities to specific project KPIs. The present deliverable provides the achieved results on enhancing awareness and training capabilities and the development of cybersecurity skills, which is 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	>6764* + 2195** = 8959
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	>80000 (Higher reach of a post)

Table 2: 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 number 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.

Built sustained collaboration with academic, industrial, governmental and community stakeholders, which is 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	> 8	> 24	> 17	> 36	40
	> 20	> 30	> 20	> 120	> 50	> 120

Table 3: Contribution to the KPIs of objective 3

2.4 Cyber Competence Network

During the period M24 – M36, the Cyber Competence Network Communication's Group was chaired by CONCORDIA project (from January 2021 until June 2021), ECHO project (from July 2021 until January 2022) and SPARTA project (from January 2022 until June 2022). During this period, WP12 was actively participating in the communication activities, namely by sending monthly contents to keep the CCN website and twitter account updated, enabling the engagement of the CCN audience. WP12 was also participating in the design of the CCN Focus Group activities, and in its communication through the SPARTA social media channels.

The regular meetings, both with the Pilots Coordinators, and within the CCN communication working-group – created to contribute specifically for joint communication and dissemination activities – continued during this period.



Figure 1: CCN at FIC 2021

On September 2021, the four pilots participated in the FIC 2021 event to present to the attendees their joint and collaborative work to strengthen Europe's cybersecurity and place Europe in a leading position in cybersecurity, through the creation of the Cybersecurity Competence Network.

From the 1st to the 3rd of June 2022, the four pilots conducted the second edition of the CONVERGENCE event: CONVERGENCE NEXT. Under the coordination of ECHO project, this event welcomed high-level representatives from EU institutions to discuss the role of the European Cybersecurity Competence Centre (ECCC) and that of the wide stakeholder community in the next stages. It focused on the future of the cybersecurity community, the ECCC and addressed cybersecurity key issues in the future.

Chapter 3 Communication and Dissemination actions

Chapter 3 reports and evaluates the actions developed by the SPARTA partners during the third year of the project conducted to disseminate and communicate project's aims, values, and results. These actions range mainly from participation and organization of events, conferences, and workshops to scientific publications. The actions designed for the third year of the project related to Tasks 12.4 and 12.5 – *Closing the Gender and Diversity Gap* and *Engagement of the Outermost Regions of Europe* – are addressed in deliverable 12.6 and 12.7, respectively. In any case, they will shortly be summarized here.

3.1 Conferences, workshops and other events

Since March 2020, the COVID-19 pandemic imposed several changes on the strategic actions planned for the second and the third year of the project, namely the on-site events. During the third year of the project and its extension period, partners - as the rest of Europe - became more resilient to the impacts caused by the pandemic and duly adapted to the new circumstances, easing the organization of and participation at events. Still, some of the events planned had to be cancelled or rescheduled. Most of the events were online, which caused roadblocks for networking and creating new collaborations.

During the three years of the SPARTA project, partners participated in 89 conferences, workshops, talks and others, organized 30 conferences and 40 Monthly Workshops, through both virtual platforms and on-site events. Most of these events occurred at the international level, and gathered a significant diversity of stakeholders, from industry to research and academy. These activities gathered and reached, in total, more than 9000 attendees. The following table reports all the events attended to or organized during the three years of the project.

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
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 30 attendees
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 35 attendees
3.	Participation to other events	CEA	SPARTA booth at DigiHall Days	Palaiseau, France	Presentation of SPARTA to the attendees of DigHall days	National 40 attendees
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 120 attendees
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 150 attendees
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 then thoroughly active this session has addressed how each pilot was planning to address the following issues: Cyber-ranges; Threat intelligence; Certification; Cybersecurity skills	International 200 attendees

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
7.	Participation to other events	CEA	Common website for pilots launch	Brussels, Belgium	<p>Welcome from CONCORDIA coordinator and introduction of new project partners, Prof. Dr. Gabi Dreo, Research Institute Cyber Defence (CODE)</p> <p>Panel discussion – True European Cooperation: a Pillar of Digital Sovereignty? Presentation of four pilots - CONCORDIA, SPARTA, ECHO and CyberSec4Europe</p> <p>Launching of the common web site</p>	International
8.	Participation to a Workshop	NCSR	H2020 Ghost clustering workshop	Athens, Greece	This workshop was 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 50 attendees
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 80 attendees
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 60 attendees
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	CEA	SPARTA Project	Palaiseau, France	Presentation of SPARTA at CEA List General Assembly	National

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
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	Presentation 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 6 attendees
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
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

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
24.	Organisation of a Conference	PPBW	Cybercrime.1 – Technologies	Warsaw, Poland	“Cybercrime.1 – Technologies” was the first edition of conferences on modern technologies and good practices used in preventing and combating cybercrime. The event consisted of a panel discussion and a workshop that provided an opportunity for participants to exchange experiences and broaden their knowledge on cybersecurity.	International 130 attendees
25.	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 200-300 attendees
26.	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 120 attendees
27.	Participation to a Conference	SAP	Heise devSec	Heidelberg, Germany	Developer conference organized by Heise/dpunkt, during which Eclipse Steady was presented.	International 290 attendees
28.	Participation to a Conference	SAP	TechEd	Barcelona, Spain	Industry conference organized by SAP, during which Eclipse Steady was presented.	International 50 attendees
29.	Participation to a Conference	SAP	EclipseCon	Ludwigsburg, Germany	Developer conference organized by the Eclipse Foundation, during which Eclipse Steady was presented.	International 50 attendees
30.	Participation to a Conference	TEC	XIII Congreso Internacional de	Madrid, Spain	https://www.cci-es.org/web/cci/detalle-congreso-/journal_content/56/10694/850611	International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
			Ciberseguridad Industrial en Europa			250 attendees
31.	Participation to a Conference	TEC	Congreso Protección de Datos Bilbao Wolters Kluwer	Bilbao, Spain	https://tienda.wolterskluwer.es/p/congreso-privacidad-bilbao	International 150 attendees
32.	Participation to a Conference	TEC	IT.SA The IT Security Expo and Congress	Nurember, Germany	https://www.it-sa.de/en	International 6.500 attendees
33.	Participation to a Conference	TEC	Congreso Basque Industry 4.0 and Basque Cybersecurity Day	Bilbao, Spain	https://agenda.spri.eus/meetingpoint/es	International 3.500 attendees
34.	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
35.	Organisation of a Workshop	CNIT	CY4GAMES	Rome, Italy	https://www.cy4gate.com/cy4games	International
36.	Participation to a Conference	CNIT	NETSOFT 2019	Paris, France	https://netsoft2019.ieee-netsoft.org/	International
37.	Participation to a Conference	LIST	ICT Spring 2019	Luxembourg	https://www.ictspring.com	International
38.	Participation to a Conference	LIST	Information Security Day 2019	Luxembourg	https://securitymadein.lu/events/information-security-day/	International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
39.	Participation to a Conference	LIST	Luxembourg Internet Days 2019	Luxembourg	https://www.luxembourg-internet-days.com	International
40.	Participation to a Conference	BUT	14th International Conference on Availability, Reliability and Security	Canterbury, United Kingdom	https://2019.ares-conference.eu/	International
41.	Participation to a Conference	BUT	13th International Conference on Network and System Security	Sapporo, Japan	http://nsclab.org/nss2019/	International
42.	Participation to a Conference	BUT	ICT Systems Security and Privacy Protection	Lisbon, Portugal	https://www.ifipsec.org/2019/	International
43.	Participation to a Conference	TNK	16. Österreichischer IT-Sicherheitstag 2019	Klagenfurt, Austria	https://www.syssec.at/de/veranstaltungen/sitag2019	International
44.	Participation to a Conference	IST	OutGene: Detecting Undefined Network Attacks with Time Stretching and Genetic Zoom	Sapporo, Japan	http://www.nsclab.org/nss2019/	International
45.	Participation to a conference	BUT	NSS 2019	Sapporo, Japan	Presentation of WP6 results: MALINA, L.; SRIVASTAVA, G.; DZURENDA, P.; HAJNÝ, J.; RICCI, S. A Privacy-Enhancing Framework for Internet of Things Services. In 13th International Conference on Network and System Security. Lecture Notes in Computer Science. Springer,	International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
					2019. s. 77-97. ISBN: 978-3-030-02744-5. ISSN: 0302-9743.	
46.	Participation to a Conference	BUT	ARES 2019	Canterbury, UK	Presentation of WP6 results: MALINA, L.; SRIVASTAVA, G.; DZURENDA, P.; HAJNÝ, J.; FUJDIK, R. A Secure Publish/Subscribe Protocol for Internet of Things. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES 2019). Canterbury, United Kingdom: ACM, 2019. s. 1-10. ISBN: 978-1-4503-7164-3.	International
47.	Participation to a Conference	IST	Omega: a Secure Event Ordering Service for the Edge	Web		International
48.	Participation to a Conference	IST	Go With the Flow: Clustering Dynamically-Defined NetFlow Features for Network Intrusion Detection with DYNIDS	Web		International
49.	Participation to a Conference	IST	Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection	Web		International
50.	Participation to a Conference	IST	CryingJackpot: Network Flows and Performance	Web		International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
			Counters against Cryptojacking			
51.	Participation to a Conference	LKA	NATO Strategic Communications Centre of Excellence annual presentation "Influence campaigns in the digital environment" in Riga	Riga	LKA participated at NATO Strategic Communications Centre of Excellence annual presentation „Influence campaigns in the digital environment" in Riga	International
52.	Participation to other events	CESNET	C2S2 2019	Milovy, Czech Republic	Meeting with national cybersecurity community	National 34 attendees
53.	Participation to a Conference	CEA	SPARTA Presentation at Forum Cybersécurité et Stratégie organisé par CEIS	Paris, France	Cybersecurity Forum	National 100 attendees
54.	Participation to other conferences	CEA	Visit of the Ministry of Interior, Police Prefecture, and Ecole Nationale Supérieure de Police at CEA.	Gif-sur-Yvette, France		National 20 attendees
55.	Participation to a Workshop	CEA	SATE VI Experience Workshop	Mclean, VA, United States	Workshop about the usage of sound static analysis tools (including Framac) in the industry, with applications both in safety and security. The event was preceded by a Software and Supply Chain Assurance Forum meeting, discussing strategic questions of cybersecurity in the software supply chain.	International 50 attendees

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
56.	Participation to a Conference	CEA INOV	Cybertech	Rome, Italy	Sparta Stand during the Sparta Event at Cybertech	International
57.	Participation to a Conference	TEC	SPARTA CAPE	Web	https://www.youtube.com/watch?v=cU1QsdyaNXs&feature=youtu.be	International
58.	Participation to a Conference	CEA	CONCORDIA Open Door	Luxembourg	Participation to a panel	International 60 attendees
59.	Participation to a Conference	CEA	European Cyberweek	Rennes, France	European Cybersecurity Week, yearly event in Rennes, (2000 visitors in 2018). Presentation of SPARTA as part of a Research and Innovation thematic.	National 80 attendees
60.	Participation to a Conference	CEA	Journée Tech Cybersécurité UTAC CERAM	Linas-Monthléry, France	Journée Tech Cybersécurité UTAC CERAM	National
61.	Participation to a Conference	CEA	High Level Forum	Grenoble, France	Speaker at the High Level Forum	National
62.	Participation to a Conference	CEA	ISO Strategic Forum, Roundtable	Paris, France	Organised with ISO/IEC JTC1/SC 27 “Sécurité de l’information, cybersécurité et protection de la vie privée” participation at a round table during the Strategic Forum	National
63.	Participation to a Conference	TEC	SPARTA “Hacia em nuevo escenario de la I+em en Ciberseguriemd en "uropa"	León, España	https://www.incibe.es/enise	International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
64.	Participation to a Conference	UTARTU	CAISE 2020	France		International
65.	Participation to a Conference	CEA	Information session on Public Private Partnerships in the light of the proposal for a Cybersecurity Competence Center	Brussels, Belgium	Presentation at "Information session on Public Private Partnerships in the light of the proposal for a Cybersecurity Competence "enter"	International
66.	Participation to a Conference	CE'	OECD's Global Forum on Digital Security for Prosperity	London, UK	Round table a' OECD's Global Forum on Digital Security for Prosperity	International
67.	Participation to a Workshop	CEA	ECISO WG6 meeting	Brussels, Belgium		International
68.	Participation to a Conference	CEA	Data Natives	Berlin, Germany	Presentation of the 4 pilots to the Council of the EU	International
69.	Participation to other events	CEA	Presentation to the Director of the French Cybersecurity Grand Challenge	Paris, France		National
70.	Participation to a Workshop	CEA	Presentation at "Workshop with Member States about the Network of National Coordination Centres"	Brussels, Belgium		International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
71.	Participation to a Conference	CEA	Forum International de la Cybersécurité	Lille, France	SPARTA Stand	International 1200 attendees
72.	Participation to a Conference	JR	SEREN4 Cybersecurity Workshop	Web	SEREN4 Cybersecurity Workshop, 28th April - ONLINE WORKSHOP on Cybersecurity, Panel discussion: The perspective of the Cybersecurity Competence Network (4 pilots) and future collaboration opportunities (http://www.seren-project.eu/) (Agenda: https://seren4-h2020-sc7-2020-infoday.b2match.io/agenda?session=52674)	International
73.	Participation to a Workshop	BUT	Workshop on Skills Framework	Web	Workshop for other pilots and ENISA on SPARTA Cybersecurity Skills Framework	International 10 attendees
74.	Participation to other events	CEA	List General Assembly	Saclay, France		International 500 participants
75.	SPARTA Event	CEA	SPARTA DAY and SPARTA meeting	Brussels, Belgium		International 70 participants
76.	Other	CEA	SPARTA Presentation	Web	French Ministry of Research pitch	National 3 attendees
77.	Other	CEA	SPARTA Presentation	Saclay, France	French Ministry of Research pitch	National 10 attendees

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
78.	Participation to other events	CNR	SPARTA Brokerage Event	Web	Brokerage event in preparation of the 08/2020 calls	International 70 attendees
79.	Participation to other events	CEA	SPARTA Presentation	Web	Presentation of SPARTA to ETP4HPC leadership	National 5 attendees
80.	Participation to a Conference	LEO	Cybertech Live	Web		International >100
81.	Participation to other events	CEA	SPARTA Presentation	Web	IFIP Sec Conference, Workshop Session on CCN	International 20 attendees
82.	Participation to a Conference	CEA	SPARTA Presentation	Web		International
83.	Moderation of panel discussion and participation to a Workshop	JR	Cybersecurity in Finance	Web		International
84.	Participation to a conference	Fraunhofer	"Taking cybersecurity forward by building competence centres"	Brussels, Belgium	Panel at CANVAS Project Final Event: Value-driven Cybersecurity: Which Security? Whose Values?	International
85.	Participation to a Workshop	JR	Cyber Security in Österreich 2020: Ein- & Ausblicke für Studierende	Web		International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
86.	Participation to a Conference	JR	GRAZ SECURITY DAYS FOR INDUSTRY 2019	Graz, Austria		International
87.	Participation to a Workshop	JR	9. Arbeitssitzung der Cyber Security Plattform Austria	Loipersdorf, Austria		International
88.	Brokerage event	JR	FORTE und KIRAS Einreichertag (National Security and Defence research programs)	Vienna, Austria		International
89.	Participation to a Conference	JR	MILIPOL Paris 2019, Workshop on AI for LEAs	Paris, France		International
90.	Brokerage event	JR	SMI2G Meeting 2020	Brussels, Belgium		International
91.	Participation to a Conference	JR	KIRAS Fachtagung (National security research program)	Vienna, Austria		International
92.	Business meeting	JR	Business meeting with Austrian supplier platformttform, stakeholder from industry –SME) - NDA!	Austria		International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
93.	Business meeting	JR	Business meeting and lab visit at Austrian university of applied sciencee	Austria		International
94.	Business meeting	JR	Business meeting with Austrian software project company RISE	Austria		International
95.	Participation to a conference	NASK	SECURE 2020 conference	Poland		International
96.	Organisation of a conference	NASK, PPBW, BUT	SECURE 2021 conference	Online	Dedicated SPARTA panel on Cybersecurity in higher education	International 300 attendees
97.	Participation to a webinar	INOV BRN	Gender & Diversity Breakfast Webinars	Web	SPARTA was represented by Sara Ricci, a Post-Doctoral Researcher at the Brno University of Technology, on the INESC HUB <i>Gender & Diversity Breakfast Webinar</i> discussions, and addressed the importance of the role-models in gender & diversity in STEM research and technology.	International
98.	Participation to a Webinar	CNR	WEBINAR: European Cybersecurity Challenges	Web		
99.	Participation to a Webinar	UKON, SAP	VizSec 2021	Online		
100.	Source Code Release	UKON, SAP		Online	https://github.com/dbvis-ukon/vulnex	International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
			VulnEx			
101.	Participation	TEC	Cybersecurity in Automotive domain	Online	Workshop on Cybersecurity at University of Ávila (Spain) about basic knowledge on cybersecurity on automotive domain. Relationship between system safety and system cybersecurity.	National 5 attendees
102.	Organisation of workshop	BUT, IMT, SMILECIN I, L3CE	ARES ETACS Workshop	Online	Workshop, panel session, invited talks	International
103.	Participation to a conference	ITTI	IDEAL	Manchester, UK	Presentation: "The Feasibility of Deep Learning Use for Adversarial Model Extraction in the Cybersecurity Domain"	International
104.	Participation to a conference	ITTI	ICCS2020	Online	Presentation: "On the Impact of Network Data Balancing in Cybersecurity Applications", Presentation: "Machine Learning – The Results Are Not the only Thing that Matters! What About Security, Explainability and Fairness?"	International
105.	Participation to a conference	ITTI	PP-RAI	Glasgow, UK	Presentation: "Achieving Explainability of Intrusion Detection System by Hybrid Oracle-Explainer Approach"	International
106.	Participation to a conference	ICCCI2021		Kalitheia, Rhodes, Greece	Presentation: "The Proposition of Balanced and Explainable Surrogate Method for Network Intrusion Detection in Streamed Real Difficult Data"	International
107.	Panelist in workshop	JR	Digitaldialog on Cybersecurity	Graz, Austria	Workshop, panel discussion, invited talks	National 30 attendees

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
108.	Organisation of a Conference	PPBW	Modern technologies and methods of criminal analysis used by law enforcement agencies to combat crime	Jurata, Poland		International 170 attendees
109.	Organisation of a Conference	PPBW	Safe E-commerce Conference (SEC)	Bedlewo, Poland	The conference was devoted to the problem of increasing number of crimes related to development of electronic commerce (e-commerce). The main idea of the conference is to discuss among practitioners how to effectively prevent and detect new threats, also in the aspect of international cooperation. The conference will bring together law enforcement agencies, prosecutors, judges and institutions directly involved in e-commerce (Internet sales platforms, banks, courier companies).	International 100 attendees
110.	Organisation of a workshop	INOV	SPARTA: The Future Needs You	Caldas da Rainha, Portugal	“SPARTA: The Future Needs You”, was an event promoted by INOV and the Brno University of Technology, for celebrating the cybersecurity awareness month and calling for diversity in the field, held in the High School of Caldas Da Rainha - Escola Secundaria Rafael Bordalo Pinheiro - in Portugal, on the 14h October	National 90 attendees
111.	Organisation of a workshop	INOV BUT	Go Cyber with SPARTA	Las Palmas de Gran Canaria, Spain	Workshop developed within the “Go Cyber with SPARTA” campaign, deployed to the University of Las Palmas de Gran Canaria, on how to use the education cybersecurity map and the cybersecurity curricula designer for the creation of a cybersecurity course	National 4 attendees

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
112.	Organisation of a workshop	INOV	Go Cyber with SPARTA - Raising Cybersecurity Awareness across the world	Madeira, Portugal	Workshop developed within the “Go Cyber with SPARTA” campaign, deployed to the SMEs on the tourism sector, about the cybersecurity for SMEs.	National 31 attendees
113.	Organisation of a workshop	INOV BUT	Go Cyber with SPARTA	La Reunion, France	Workshop developed within the “Go Cyber with SPARTA” campaign, deployed to the Office de l’eau employees – Water critical infrastructure – about cybersecurity in context of critical infrastructures.	National 4 attendees
114.	Organisation of a workshop	INOV BUT	Go Cyber with SPARTA	La Reunion, France	Workshop developed within the “Go Cyber with SPARTA” campaign, deployed to SMEs in the digital sector, from La Reunion.	National 14 attendees
115.	Organisation of a workshop	SMILE	SPARTA Hackathon I	Online	SPARTA Cybersecurity Hackathon aimed at identifying and designing solutions to some of the recurring problems or come up with entirely new solutions which would take cybersecurity to the next level.	International 50 attendees
116.	Organisation of a workshop	SMILE	SPARTA Hackathon II	Belval, Luxembourg	Business Development Hackathon for building products from available cybersecurity open-source tools. Up to 12 teams compete and use tools developed under SPARTA and CONCORDIA.	International 50 attendees
117.	Organisation of a workshop	CEA, INOV	CONVERGENCE EVENT	Brussels, Belgium	Focused upon the future of ECCC and looked at the key issues for cybersecurity in the future.	International N/A
118.	Organisation of a workshop	CEA	Sparta days	Paris, France	Wrap-up/ conclusion event of the SPARTA project	International 67

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
119.	Participation at an event	INOV	PPHS event	Poland	SPARTA presented project results on cybersecurity for Law Enforcement Authorities	National 80 attendees
SPARTA Monthly Workshops						
120.	Organisation	CEA		France	Held during the SPARTA Kick Off meeting	International 120 attendees
121.	Organisation	LEO		Italy	Held during the Cybertech Europe Event	International 120 attendees
122.	Organisation	CNR		Italy	Held during Cybersecurity Day	International 240 attendees
123.	Organisation	UBO		Bonn, Germany	Held during BDCS	International
124.	Organisation	L3C		Vilnius, Lithuania	The objective of the workshop was to disseminate the SPARTA goals and results between national stakeholders and promote international collaboration and networking.	International
125.	Organisation	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 32 attendees

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
126.	Organisation	YWH	Mundo Hacker 6 th Edition	Madrid, Spain	Presentation of SPARTA and TSHARK during the conference	International 50 attendees
127.	Organisation	VICOM TEC EUT IND	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 19 attendees
128.	Organisation	CETIC		Brussels, Belgium SPARTA WEEK		International 30 attendees
129.	Organisation	UTARTU	Tartu Security initiative meetings	Online, Estonia	The main goal of these meetings is to assemble the parties who are interested in the Cybersecurity research and development in Tartu (Estonia). The meeting attracted the Cybersecurity research group representatives from the University of Tartu, Startup Estonia, Defence League members, ISACA Estonia representatives and private companies (e.g., Cybernetica, Guardtime, etc.)	National 28 attendees
130.	Organisation	YWH		Paris, France	co-located with Paris Cyber Week	National
131.	Organisation	YWH		Paris, France	Masterclass Sciences Po	National
132.	Organisation	CNR + Swisscore		Switzerland		National

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
						140 attendees
133.	Organisation	CETIC AND Leonardo Cybersecurity	First international workshop on lightweight and incremental cybersecurity certification	Online	https://www.ieee-security.org/TC/EuroSP2020/	International
134.	Organisation	LMT - L3CE		Vilnius, Estonia		International
135.	Organisation	Fraunhofer and CS4E	IFIP Summer School on Privacy and Identity Management	Online	<p>This Summer School is a joint effort between the IFIP Working Groups 9.2, 9.6/11.7, 11.6, and Special Interest Group 9.2.2 and different European and national research projects. The 2018 IFIP Summer School will bring together junior and senior researchers and practitioners from multiple disciplines to discuss important questions concerning privacy and identity management and related issues in a global environment subject to change. This Summer School is not a “taught course”: it does enable, however, students to gain credit points for presenting and attending, and their paper to be considered as a candidate for a Best Paper award.</p> <p>The original plan was to hold a physical 1-week summer school in Brno (hosted by BUT). Virtual event is a partial replacement. Original concept will be implemented in 2021</p>	International 35 attendees
136.	Organisation	SPARTA		Brussels,		International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
				Belgium		
137.	Organisation	MRU, Fraunhofer, CEA, CANVAS, CONCORDIA	Workshop on Ethical, Societal and Legal Questions in Cybersecurity Research	Online		International
138.	Organisation	CINI		Genova, Italy		International
139.	Organisation	CNR		Pisa, Italy		International
140.	Organisation	INRIA		Léon, Spain		International
141.	Organisation	UTRATU	SPARTA workshop at Baltic DB&IS 2020	Tartu, Estonia	To discuss with policymakers, academics and foremost small and medium-sized companies needs and challenges of Baltic Sea region, scan other EU regions for solutions and propose new ideas dedicated to experience, knowledge, skills and long-lasting partnerships. To demonstrate how SPARTA partnership program can be designed to overcome the barriers that single players face in Cybersecurity market.	International
142.	Organisation	L3CE	-	Virtual	-	International 30 attendees

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
143.	Organisation	SMILE	https://sparta.eu/events/2020-12-09-sparta-workshop-how-to-get-privileged-access-to-groundbreaking-cybersecurity-innovations-and-research.html	Virtual	SPARTA Workshop: How to get privileged access to ground-breaking Cybersecurity innovations and research?	International 27 attendees
144.	Organisation	SMILE		Luxemburg		National 28 attendees
145.	Organisation	KEMEA		Online, Greece		National
146.	Organisation	CESNET		Prague, Czech Republic	during CESNET conference	International 94 attendees
147.	Organisation	INOV	Cybersecurity Challenges for SME's	Lisboa, Portugal	INOV in partnership with Instituto Superior Técnico and with the support of AIDA-Chamber of Commerce and Industry of the District of Aveiro is pleased to invite you to the webinar "Cybersecurity Challenges for SMEs" on January 21st, at 5:30 pm	National 21 attendees
148.	Organisation	TEC and EUT	Evaluation workshop of the TEC Demonstrator in CAPE Vertical 1	Spain	https://www.sparta.eu/news/2021-09-17-evaluation-of-the-cooperative-car-demonstrator-developed-by-tecnalia-in-the-cape-program.html	International 5 attendees
149.	Organisation	LMT		Latvia, online	Co located with cyberchess	International

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
150.	Organisation	CNR		Pisa, Italy		International 80 Attendees
151.	Organisation	SMILE		Luxembourg , Virtual		International 50 Attendees
152.	Organisation	L3C		Online		International, 35 attendees
153.	Organisation	CETIC	CyberSert 2021	Online	Second International Workshop on Cybersecurity Certification IEEE EuroS&P 2021 all-digital conference	International 24 attendees
154.	Organisation	ALL	SPARTA DAY BROKERAGE EVENT	Online		International 120 attendees
155.	Organisation	LMT, CEA, CNR, TUM	SPARTA online workshop during the International Scientific Conference	Online	https://innovations.lmt.lv/en/news/lmt-organizes-sparta-online-workshop-during-the-international-scientific-conference	International
156.	Organisation	CNR IMT	SPARTA workshop - Fosad school	Bertinoro/hybrid, Italy		International 30 attendees
157.	Organisation	CNR IMT	SPARTA workshop - transport	Bertinoro/hybrid,		International 50 attendees

	Type of activities	Main leader	Title	Place	Description of the event	National/ Inter.
				Italy		
158.	Organisation	UTARTU BUT	ARES SP2I workshop	Teleconference	Workshop, panel session, invited talks	International 30 attendees
159.	Organisation	BUT	National Cybersecurity Platform	Brno, Czech Republic	Workshop, panel session, invited talks	National 45 attendees
160.	Organisation	YWH	SPARTA monthly workshop at “Hack Me, I’m famous” event	Paris, France	Alongside the live Bug Bounty, the workshop gathered the European ethical community to discuss their contribution to the European cybersecurity.	International

Table 4: Updated and final list of the SPARTA events

*A more detailed report on the SPARTA Monthly Workshops can be found in the deliverable *D8.2 Intermediate results of the Clustering, platforms and ecosystems activities, DEM, PU, M24, VICOM: This deliverable presents the results of all the WP8 monthly workshops in M24.*

3.2 Scientific Publications

In this section is highlighted the list of accepted SPARTA scientific publications. The SPARTA partners published, in total, 128 scientific papers under the SPARTA project. The SPARTA website [Results](#) page, where the scientific publications are stored and organised to facilitate the search process, allows for more acute dissemination of these contents. Through this page link, one can share the papers on the SPARTA social media platforms (LinkedIn, and Twitter).

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
1.	Formal Security Verification of Industry 4.0 Applications	Vivek Nigam and Carolyn Talcott	ETFA	http://nigam.info/docs/etfa19.pdf	Cited by 10 (Google Scholar 12, 2021), 126 downloads
2.	Fast Keyed-Verification Anonymous Credentials on Standard Smart Cards	Jan Camenisch and Manu Drijvers and Petr Dzurenda and Jan Hajny	ICT Systems Security and Privacy Protection - IFIP SEC 2019	https://eprint.iacr.org/2019/460.pdf	Cited by 18 (Google Scholar 12, 2021), 840 downloads
3.	A Secure Publish/Subscribe Protocol for Internet of Things	Lukas Malina, Gautam Srivastava, Petr Dzurenda and Jan Hajny	ARES 2019	http://nigam.info/docs/etfa19.pdf	Cited by 49 (Google Scholar 12/2021), 319 Downloads CORE B
4.	Security Risk Management in Cooperative Intelligent Transportation Systems: A Systematic Literature Review	Abasi-amefon O. Affia, Raimundas Matulevičius, Alexander Nolte	27th International Conference on Cooperative Information Systems	https://www.researchgate.net/profile/Raimundas-Matulevicius/publication/336770438_Security_Risk_Management_in_Cooperative_Intelligent_Transportation_Systems_A_Systematic_Literature_Review/links/600aaf345851553a0606648/Security-Risk-Management-in-Cooperative-Intelligent-Transportation-Systems-A-Systematic-Literature-Review.pdf	Cited by 3 (Google Scholar 12/2021) 1,4K Downloads CORE A
5.	CFI: Control Flow Integrity or Control Flow Interruption?	Paolo Prinetto and Gianluca Roascio	PHISIC 2019 Workshop	10.1109/EWDTS.2019.884464	Cited by 6 (Google Scholar 12/2021), 252 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
6.	Experimental analysis of the laser-induced instruction skip fault model	Jean-Max Dutertre, Timothe´ Riom, Olivier Potin, and Jean-Baptiste Rigaud	2019 FDTC workshop	https://hal.archives-ouvertes.fr/hal-02379754/document	Cited by 14 (Google Scholar 12/2021), 579 downloads
7.	Big Data Analytics for Intrusion Detection: An Overview	Luis Dias, Miguel Correia	13th International Conference on Network and System Security	https://www.gsd.inesc-id.pt/~mpc/pubs/Big_Data_Analytics_for_Intrusion_Detection_An_Overview_final.pdf	Cited by 6 (Google Scholar 12/2021), NA downloads
8.	OutGene: Detecting Undefined Network Attacks with Time Stretching and Genetic Zooms	Luís Dias, Hélder Reia, Rui Neves and Miguel Correia	13th International Conference on Network and System Security	https://www.gsd.inesc-id.pt/~mpc/pubs/OutGene_Detecting_Undefined_Attacks_without_Training_Data.pdf	Cited by 3 (Google Scholar 12/2021), 1,2k downloads CORE B
9.	Visual Analytics for Cyber Security Domain: State-of-the-Art and Challenges	R. Damaševičius, J. Toldinas, A. Venčkauskas, S. Grigaliūnas, N. Morkevičius, V. Jukavičius	International Conference on Information and Software Technologies	https://doi.org/10.1007/978-3-030-30275-7_20	Cited by 2 (Google Scholar 12/2021), 744 downloads CORE B
10.	The feasibility of Deep learning use for adversarial model extraction in the cybersecurity domain	Pawlicki, Choras and Kozik	IDEAL'19	10.1007/978-3-030-33617-2_36	Cited by 5 (Google Scholar 12/2021), 647 downloads CORE C
11.	On Computer - Aided Techniques for Supporting	Vivek Nigam, Antonaneta Kondeva, Carmen	9 th IEEE International Workshop on	http://nigam.info/docs/workshop2002.pdf	Cited by 5 (Google Scholar 12/2021), 89 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	Safety and Security Co-Engineering	Carlan and Harald Ruess	Software Certification (WoSoCer)		
12.	Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols	Guillaume Celosia, Mathieu Cunche	PoPETs2020	10.2478/popets-2020-0003	Cited by 24 (Google Scholar 12/2021), NA downloads
13.	Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile	Guillaume Celosia, Mathieu Cunche	IoT S&P 2019	10.1145/3338507.3358617	Cited by 13 (Google Scholar 12/2021), 309 downloads
14.	Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism	Guillaume Celosia, Mathieu Cunche	Mobiquitous 2019	10.1145/3360774.3360777	Cited by 18 (Google Scholar 12/2021), 135 downloads
15.	Towards formal verification of IoT protocols: A Review	Katharina Hofer-Schmitz, Branka Stojanovi	Computer Networks 2020	https://doi.org/10.1016/j.comnet.2020.107233	Cited by 16 (Google Scholar 12/2021), 135 downloads
16.	Automated Security Analysis of IoT Software Updates	Nicolas Dejon, Davide Caputo, Luca Verderame, Alessandro Armando and Alessio Merlo	13th WISTP International Conference on Information Security Theory and Practice	https://csec.it/papers/WISTP2019.pdf	Cited by 3 (Google Scholar 12/2021), NA downloads
17.	Natural Projection as Partial Model Checking	Costa, G.; Galletta, L.; Degano, P.; Basin, D.; Bodei, C.	Journal of Automated Reasoning	https://arpi.unipi.it/handle/11568/1013170	Cited by 0 (Google Scholar 12/2021), 343 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
18.	WAF-A-MoLE: An adversarial tool for assessing ML-based WAFs	Luca Demetrio, Gabriele Costa, Andrea Valenza and Giovanni Lagorio	SoftwareX and on ACM Symposium on Applied Computing	https://doi.org/10.1016/j.softx.2019.100367	Cited by 1 (Google Scholar 12/2021), 11 downloads
19.	A Survey on Multi-Factor Authentication for Online Banking in the Wild	Federico Sinigaglia, Roberto Carbone, Gabriele Costa, Nicola Zannone	Computers and Security	https://doi.org/10.1016/j.cose.2020.101745	Cited by 17 (Google Scholar 12/2021)
20.	Building Next Generation Cyber Ranges with CRACK	Enrico Russo, Gabriele Costa, Alessandro Armando	Computers and Security	https://doi.org/10.1016/j.cose.2020.101837	Cited by 12 (Google Scholar 12/2021)
21.	Secure Firmware Updates for Constrained IoT Devices Using Open Standards: A Reality Check	K. Zandberg, K. Schleiser, F. Acosta, H. Tschofenig, and E. Baccelli	IEEE Access, June 2019	10.1109/ACCESS.2019.2919760	Cited by 42 (Google Scholar 12/2021)
22.	Cyberphysical Security for the Masses: A Survey of the Internet Protocol Suite for Internet of Things Security	H. Tschofenig, E. Baccelli	IEEE Security & Privacy, October 2019	https://hal.inria.fr/hal-02351892/document	Cited by 26 (Google Scholar 12/2021)
23.	Requirements for a Lightweight AKE for OSCORE	M. Vucinic, G. Selander, J. Mattsson, D. Garcia	IETF Internet Draft, 2019	https://tools.ietf.org/id/draft-selander-lake-reqs-02.html	Cited by 5 (Google Scholar 12/2021)

Nº	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
24.	Advances in Usability of Formal Methods for Code Verification with Frama-C	André Maroneze, Valentin Perrelle, Florent Kirchner	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	Cited by 0 (Google Scholar 12/2021)
25.	Privacy-preserving and yet Robust Collaborative Filtering Recommender as a Service	Qiang Tang	Inscript 2019	https://arxiv.org/abs/1910.03846v1	Cited by 11, NA downloads
26.	A Privacy-Enhancing Framework for Internet of Things Services	Lukas Malina, Gautam Srivastava, Petr Dzurenda, Jan Hajny and Sara Ricci	13th International Conference on Network and System Security	https://eprint.iacr.org/2019/1471.pdf	Cited by 19 (Google Scholar 12/2021), 1.4k Downloads, CORE B
27.	xMP: Selective Memory Protection for Kernel and User Space	Sergej Proskurin, Marius Momeu, Seyedhamed Ghavamnia, Vasileios P. Kemerlis, and Michalis Polychronakis	2020 IEEE Symposium on Security and Privacy (SP), 2020, pp. 563-577	DOI: 10.1109/SP40000.2020.00041	Cited by 17 (Google Scholar 12/2021) 679 downloads
28.	TSNSCHED: Automated Schedule Generation for Time Sensitive Networking	Aellison Cassimiro T. dos Santos, Ben	FMCAD	DOI: 10.23919/FMCAD.2019.8894249	Cited by 14 (Google Scholar 12/2021), 662 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
		Schneider and Vivek Nigam			
29.	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	The WebConf 2020	https://arxiv.org/abs/2002.01656	Cited by 22 (Google Scholar 12/2021) 788 downloads
30.	Methodology and Feedback about Systematic Cybersecurity Experts Auditing in Belgium	Christophe Ponsard, Jeremy Grandclaudon and Nicolas Point	ICISSP 2020 conference	https://www.cetic.be/Metodology-and-Feedback-about-Systematic-Cybersecurity-Experts-Auditing-in	Cited by 1 (Google Scholar 01/2021)
31.	Towards Visual Debugging for Multi-Target Time Series Classification	Udo Schlegel, Eren Cakmak, Hiba Arnout, Mennatallah El-Assady, Daniela Oelke, Daniel A Keim	ACM IUI 2020	https://bib.dbvis.de/publications/view/854	Cited by 3 (Google Scholar 12/2021), 210 downloads
32.	Provably Secure Isolation for Interruptible Enclaved Execution on Small Microprocessors	Matteo Busi, Job Noorman, Jo Van Bulck, Letterio Galletta, Pierpaolo Degano, Jan Tobias Mühlberg, Frank Piessens	33rd IEEE Computer Security Foundations Symposium	arXiv:2001.10881v1	Cited by 18 (Google Scholar 12/2021), 206 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
33.	Enhancing Security in 6G Visible Light Communications	Simone Soderi	6G Wireless Summit	https://www.researchgate.net/publication/339974971_Enhancing_Security_in_6G_Visible_Light_Communications	Cited by 9 (Google Scholar 12/2021), 609 downloads
34.	Achieving Explainability of Intrusion Detection System by Hybrid Oracle-Explainer Approach	Szczepanski, Choras, Pawlicki, Kozik.	IJCNN conference	https://api.semanticscholar.org/CorpusID:221558966	Cited by 7 (Google Scholar 12/2021)
35.	Machine Learning - The results are not the only thing that matters! What about security, explainability and fairness?	Szczepanski, Choras, Pawlicki, Kozik.	ICCS 2020	https://doi.org/10.1007/978-3-030-50423-6_46	Cited by 14 (Google Scholar 12/2021), 2.3K downloads CORE A
36.	On the impact of network data balancing in cybersecurity applications	Pawlicki, Choras, Kozik and Holubowicz	ICCS 2020	https://doi.org/10.1007/978-3-030-50423-6_15	Cited by 11 (Google Scholar 12/2021), 1.2K downloads
37.	Defending Network Intrusion Detection Systems against Adversarial Evasion Attacks	Pawlicki, Choras, Kozik	FGCS (Elsevier)	https://doi.org/10.1016/j.future.2020.04.013	Cited by 32 (Google Scholar 12/2021)
38.	Foreshadow-VMM: Feasibility and Network Perspective	Marco Spaziani brunella, Sara Turco, Giuseppe Bianchi, Francesco Quaglia, Nicola Blefari Melazzi	IEEE	https://www.researchgate.net/publication/334057814_Foreshadow-VMM_Feasibility_and_Network_Perspective	Cited by 0 (Google Scholar 01/2021), 72 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
39.	Technical Threat Intelligence Analytics: What and How to Visualize for Analytic Process	R. Damasevicus, J. Toldinas, A. Venckauskas, S. Grigaliunas, N. Morkevicius	24th International Conference ELECTRONICS 2020 and for publication in the IEEE Conference Proceedings	https://doi.org/10.1109/IEECONF49502.2020.9141613	Cited by 0 (Google Scholar, 12/2021), 151downloads
40.	Towards Formal Methods of IoT Application Layer Protocols	Katharina Hofer-Schmitz, Branka Stojanovi	Proceedings of the 12th CMI conference - Cybersecurity and Privacy (CMI 2019).	DOI: 10.1109/CMI48017.2019.8962139	Cited by 7 (Google Scholar, 12/2021), 223 downloads
41.	Disconnection attacks against LoRaWAN 1.0.X ABP devices	Giorgio Bernardinetti, Francesco Mancini, Giuseppe Bianchi	IEEE MetComNet 2020 conference	http://netgroup.uniroma2.it/wp-content/uploads/2021/01/LoRaWAN-ABP-Attacks.pdf	Cited by 3 (Google Scholar, 12/2021), 94 downloads
42.	ModelSpeX: Model Specification Using Explainable Artificial Intelligence Methods	Udo Schlegel, Eren Cakmak, and Daniel A. Keim	MLVis 2020 Workshop	https://bib.dbvis.de/uploadedFiles/MLVIS_2020_ModelSpeX_Model_Specification_Using_Explainable_Artificial_Intelligence_Methods.pdf	Cited by 1 (Google Scholar, 12/2021) NA downloads Impact Score: 2.116 (Eurographics Forum)
43.	LITNET-2020: An Annotated Real-World Network Flow Dataset for Network Intrusion	Damasevicus, Robertas; Venckauskas, Algimantas; Grigaliunas,	Detection Electronics 9, no. 5: 800.	https://doi.org/10.3390/electronics9050800	Cited by 27 (Google Scholar, 12/2021) NA downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
		Sarunas; Toldinas, Jevgenijus; Morkevicius, Nerijus; Aleliunas, Tautvydas; Smuikys, Paulius.			
44.	Borrowing Your Enemy's Arrows: the case of Code Reuse in Android via Direct Inter-app Code Invocation	Jun Gao, Li Li, Pingfan Kong, Tegawendé F. Bissyandé and Jacques Klein	28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering	https://jacquesklein2302.github.io/papers/2020-jun-gao-FSE.pdf	Cited by 6 (Google Scholar, 12/2021) NA downloads
45.	Cybersecurity Certification for Agile and Dynamic Software Systems – a Process-Based Approach	Volkmar Lotz	CyberCert 2020	https://conferences.computer.org/eurosp/pdfs/EuroSPW2020-7k9FIVRX4z43j4uE2SeXU0/859700a085/859700a085.pdf	Cited by 1 (Google Scholar, 12/2021) NA downloads
46.	Towards Automating Safety and Security Co-Analysis with Patterns	Yuri Dantas, Antoaneta Kondeva, Vivek Nigam	SafeCOMP 2020	https://hal.laas.fr/hal-02931717	Cited by 0 (Google Scholar, 12/2021) NA downloads
47.	Less Manual Work for SafetyEngineers: Towards an	Yuri Dantas, Antoaneta	ICLP 2020	https://arxiv.org/abs/2009.10251	Cited by 1 Google Scholar, 12/2021), NA downloads

Nº	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	Automated Safety Reasoning with Safety Patterns	Kondeva, Vivek Nigam			
48.	MobHide: App-level Runtime Data Anonymization on Mobile	Davide Caputo, Luca Verderam, Alessio Merlo	1st International Workshop on Security in Mobile Technologies In Conjunction With ACNS 2020	https://link.springer.com/chapter/10.1007/978-3-030-61638-0_27	Cited by 2 (Google Scholar, 12/2021), 231 downloads CORE B
49.	Privacy Enhancing Technologies for solving the Privacy-Personalization Paradox	Nesrine Kaaniche, Maryline Laurent and Sana Belguith	Journal of Network and Computer Applications 2020	https://www.sciencedirect.com/science/article/abs/pii/S1084804520302794	Cited by 5 (Google Scholar, 12/2021), 746 downloads
50.	Backstabber's Knife Collection: A Review of OpenSource Software Supply Chain Attacks	Ohm, M., Plate, H., Sykosch, A., Meier, M. (2020, July)	17th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment	https://arxiv.org/abs/2005.09535	Cited by 20 (Google Scholar, 12/2021), 8.2K downloads CORE C
51.	Towards Detection of Software Supply Chain Attacks by Forensic Artifacts	Ohm, M., Sykosch, A., Meier, M. (2020, August)	15th International Conference on Availability, Reliability and Security. ACM.	https://www.researchgate.net/publication/342764646_Towards_Detection_of_Software_Supply_Chain_Attacks_by_Forensic_Artifacts	Cited by 5 (Google Scholar, 12/2021), 297 downloads CORE B
52.	Multiscale Snapshots: Visual Analysis of Temporal Summaries in Dynamic Graphs	Eren Cakmak, Udo Schlegel, Dominik Jäckle, Daniel	EEE Transactions on Visualization	https://arxiv.org/abs/2008.08282	Cited by 3 (Google Scholar, 12/2021), 272 downloads

Nº	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
		Keim, Tobias Schreck	and Computer Graphics (TVCG)		
53.	<i>dg2pix: Pixel-Based Visual Analysis of Dynamic Graphs</i>	Eren Cakmak, Dominik Jäckle, Tobias Schreck, Daniel Keim	VDS at IEEE VIS 2020	https://arxiv.org/abs/2009.07322	Cited by 1 (Google Scholar, 12/2021), 53 downloads
54.	Towards Incremental Safety and Security Requirements Co-Certification	Morgagni Andrea, Massonet Philippe, Dupont Sébastien, Grandclaudon Jeremy	CyberCert 2020 workshop	https://conferences.computer.org/eurosp/pdfs/EuroSPW2020-7k9FIVRX4z43j4uE2SeXU0/859700a079/859700a079.pdf	Cited by 1 (Google Scholar, 12/2021), 90 downloads
55.	Go With the Flow: Clustering Dynamically-Defined NetFlow Features for Network Intrusion Detection with DYNIDS	Luis Dias, Simão Valente and Miguel Correia	In Proceedings of the 19th IEEE International Symposium on Network Computing and Applications	https://www.gsd.inesc-id.pt/~mpc/pubs/Go_With_the_Flow_Clustering_Dynamically_Defined_NetFlow_Features-final.pdf	Cited by 2 (Google Scholar, 12/2021), 71 downloads CORE A
56.	Towards Quantum-Enhanced Machine Learning for Network Intrusion Detection	Arnaldo Gouveia and Miguel Correia	In Proceedings of the 19th IEEE International Symposium on Network Computing and Applications	https://www.gsd.inesc-id.pt/~mpc/pubs/Quantum_NIDS_final.pdf	Cited by 1 (Google Scholar, 12/2021) CORE A

Nº	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
57.	CryingJackpot: Network Flows and Performance Counters against Cryptojacking	Gilberto Gomes, Luis Dias and Miguel Correia	In Proceedings of the 19th IEEE International Symposium on Network Computing and Applications (NCA), Nov. 2020.	https://www.gsd.inesc-id.pt/~mpc/pubs/CryingJackpot_final.pdf	Cited by 4 (Google Scholar, 12/2021) CORE A
58.	C2BID: Cluster Change-Based Intrusion Detection	Tiago Fernandes, Luis Dias and Miguel Correia	In Proceedings of Trustcom 2020, December 2020.	https://www.gsd.inesc-id.pt/~mpc/pubs/C2BID_final.pdf	Cited by 0 (Google Scholar, 12/2021) CORE A
59.	Never Trust Your Victim: Weaponizing Vulnerabilities in Security Scanners	Andrea Valenza, Gabriele Costa, and Alessandro Armando	23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020).	https://www.usenix.org/system/files/raid20-valenza.pdf	Cited by 1 (Google Scholar, 12/2021)
60.	Challenges in Cyber Security Education	Sara Ricci, Jan Hajny, Edmundas Piesarskas, Simon Parker	CyberEDU Conference	https://www.ijisc.com/articles/2020-02-01.pdf	Cited by 1 (Google Scholar, 12/2021)
61.	Towards Automatic Identification of Typosquatting Attacks in PyPI	Duc Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, Antonino Sabetta	WACCO Workshop @ Euro S&P	No information available yet	No information available yet

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
62.	Towards Using Source Code Repositories to Identify Software Supply Chain Attacks	Duc Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, Antonino Sabetta	CCS 2020	https://www.researchgate.net/publication/345986133_Poster_Towards_Using_Source_Code_Repositories_to_Identify_Software_Supply_Chain_Attacks	Cited by 7 (Google Scholar, 12/2021), 68 downloads
63.	SEkey: A Distributed Hardware-based Key Management System	Matteo Fornero, Nicolò Maunero, Paolo Prinetto, Antonio Varriale	18th IEEE EAST-WEST DESIGN & TEST SYMPOSIUM (EWDTS-2020)	https://ieeexplore.ieee.org/document/9225107	Cited by 0 (Google Scholar, 12/2021), 56 downloads
64.	Hardware-based Capture-the-Flag Challenges	Gianluca Roascio, Paolo Prinetto, Antonio Varriale	18th IEEE EAST-WEST DESIGN & TEST SYMPOSIUM (EWDTS-2020)	https://ieeexplore.ieee.org/abstract/document/9224932	Cited by 2 (Google Scholar, 12/2021), 128 downloads
65.	A FPGA-based Control-Flow Integrity Solution for Securing Bare-Metal Embedded Systems	Nicolò Manuearo (POLITO), Gianluca Roascio (POLITO), Paolo Prinetto (Polito), Antonio Varriale (B5 Labs Ltd.)	IEEE 15th International Conference on Design & Technology of Integrated Systems (DTIS) 2020	https://ieeexplore.ieee.org/document/9081314	Cited by 5 (Google Scholar 12/2021) 223 downloads
66.	Minimal Virtual Machines on IoT Microcontrollers: The Case of Berkeley Packet Filters with rBPF	K. Zandberg, E. Baccelli	IFIP/IEEE PEMWN 2020	https://arxiv.org/abs/2011.12047	Cited by 3 (Google Scholar 12/2021) NA downloads

Nº	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
67.	Low-Power IoT Communication Security: On the Performance of DTLS and TLS 1.3	G. Restuccia, H.Tschofenig, E. Baccelli	IFIP/IEEE PEMWN 2020	https://arxiv.org/abs/2011.12035	Cited by 5 (Google Scholar 12/2021) 156 downloads
68.	Omega: a Secure Event Ordering Service for the Edge	Cláudio Correia, Luis Rodrigues, Miguel Correia	50th IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)	https://www.qsd.inesc-id.pt/~mpc/pubs/Claudio_DSN_camera_ready.pdf	Cited by 4 (Google Scholar 12/2021) 185 downloads CORE A
69.	Deep Learning for Network Intrusion Detection: An Empirical Assessment	Arnaldo Gouveia and Miguel Correia	Advances in Security, Privacy and Trust for Internet-of-Things (IoT) and Cyber-Physical Systems (CPS), 2020	https://www.qsd.inesc-id.pt/~mpc/pubs/DL-book-chapter.pdf	Cited by 2 (Google Scholar 12/2021) NA downloads
70.	Network Intrusion Detection with XGBoost	Arnaldo Gouveia, Miguel Correia	Advances in Security, Privacy and Trust for Internet-of-Things (IoT) and Cyber-Physical Systems (CPS), 2020	https://www.qsd.inesc-id.pt/~mpc/pubs/XGBoost_chapter.pdf	Cited by 1 (Google Scholar 12/2021) NA downloads
71.	A Formal Security Assessment Framework for Cooperative Adaptive Cruise Control	Yuri Gil Dantas (fortiss, Germany), Vivek Nigam (fortiss, Germany), Carolyn Talcott	2020 IEEE Vehicular Networking Conference (VNC)	http://nigam.info/docs/vnc20.pdf	Cited by 2 (Google Scholar 12/2021) 103 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
		(SRI International, USA)			
72.	An Edge-Fog Secure Self-Authenticable Data Transfer Protocol	Venčkauskas A, Morkevicius N, Jukavičius V, Damaševičius R, Toldinas J, Grigaliūnas Š.	Sensors. 2019; 19(16):3612.	https://www.mdpi.com/1424-8220/19/16/3612#cite	Cited by 13 (Google Scholar 12/2021) 1969 downloads
73.	Orchestration Security Challenges in the Fog Computing	Šatkauskas N., Venčkauskas A., Morkevicius N., Liutkevičius A.	Information and Software Technologies. ICIST 2020. Communications in Computer and Information Science, vol 1283. Springer, Cham.	https://doi.org/10.1007/978-3-030-59506-7_17	Cited by 1 (Google Scholar 12/2021) 323 downloads
74.	Revisiting the VCCFinder Approach for the Identification of Vulnerability	Timothé Riom, Arthur D. Sawadogo, Kevin Allix, Alexandre Bartel, Tegawendé F. Bissyandé, Naouel Moha and Jacques Klein	Empirical Software Engineering, journal first, Springer, Accepted for publication on Jan. 22, 2021	https://link.springer.com/article/10.1007/s10664-021-09944-w	Cited by 1 (Google Scholar 12/2021) 981 downloads CORE A
75.	A First Look at Android Applications in Google Play related to Covid-19	Jordan Samhi, Kevin Allix, Tegawendé F.	Empirical Software Engineering, journal first, Springer, Accepted	https://link.springer.com/article/10.1007/s10664-021-09943-x	Cited by 3 (Google Scholar 12/2021) 1494 downloads CORE A

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
		Bissyandé, Jacques Klein	for publication on Jan. 15, 2021		
76.	On the Impact of Sample Duplication in Machine Learning based Android Malware Detection	Yanjie Zhao, Li Li, Haoyu Wang, Haipeng Cai, Tegawendé F. Bissyandé, Jacques Klein, John Grundy	ACM Transactions on Software Engineering and Methodology (TOSEM), journal first, ACM, Accepted for publication on Jan. 07, 2021	https://doi.org/10.1145/3446905	Cited by 2 (Google Scholar 12/2021) 242 downloads CORE A
77.	Towards an Interpretable Deep Learning Model for Mobile Malware Detection and Family Identification	Giacomo Iadarola, Fabio Martinelli, Francesco, Antonella Santone	Computer & Security, 2021	https://doi.org/10.1016/j.cose.2021.102198	Cited by 7 (Google Scholar 12/2021) NA downloads
78.	Detecting Colluding Inter-App Communication in Mobile Environment	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	International Conference on Information Systems Security and Privacy, IC/ISSP 2021	https://doi.org/10.3390/app10238351	Cited by 3 (Google Scholar 12/2021) 712 downloads
79.	Neural Networks for Driver Behavior Analysis	Fabio Martinelli, Fiammetta Marulli, Francesco Mercaldo, Antonella Santone	Electronics	https://doi.org/10.3390/electronics10030342	Cited by 1 (Google Scholar 12/2021) 690 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
80.	Driver Identification through Formal Methods	Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone	IEEE Transactions on Intelligent Transportation Systems	DOI: 10.1109/TITS.2021.3055347	Cited by 0 (Google Scholar, 12, 2021), 50 downloads
81.	Call Graph and Model Checking for Fine-Grained Android Malicious Behaviour Detection	Giacomo Iadarola, Fabio Martinelli, Francesco, Antonella Santone	Applied Sciences	https://doi.org/10.3390/app10227975	Cited by 5 (Google Scholar 12/2021) 609 downloads
82.	Android Collusion: Detecting Malicious Applications Inter-Communication through Shared Preferences	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	Information	https://www.mdpi.com/2078-2489/11/6/304	Cited by 4 (Google Scholar 12/2021) 867 downloads
83.	Detecting Colluding Inter-App Communication in Mobile Environment	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	Applied Sciences	https://doi.org/10.3390/app10238351	Cited by 3 (Google Scholar 12/2021) 712 downloads
84.	Visualizing the outcome of dynamic analysis of Android malware with VizMal	Andrea De Lorenzo, Fabio Martinelli, Eric Medvet, Francesco Mercaldo, Antonella Santone	Journal of Information Security and Applications	https://doi.org/10.1016/j.jisa.2019.102423	Cited by 23 (Google Scholar 12/2021) NA downloads 2.327

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
85.	Model checking and machine learning techniques for HummingBad mobile malware detection and mitigation	Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone, Gigliola Vaglini	Simulation Modelling Practice and Theory	https://doi.org/10.1016/j.simpat.2020.102169	Cited by 5 (Google Scholar 12/2021) 712 downloads
86.	VisualDroid: automatic triage and detection of Android repackaged applications	Rosangela Casolare, Carlo De Dominicis, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	15th International Conference on Availability, Reliability and Security (ARES)	https://dl.acm.org/doi/10.1145/3407023.3407074	Cited by 3 (Google Scholar 12/2021) 65 downloads CORE B
87.	Colluding Android Apps Detection via Model Checking	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone	Web, Artificial Intelligence and Network Applications	https://link.springer.com/chapter/10.1007/978-3-030-44038-1_71	Cited by 4 (Google Scholar 12/2021) 1.3K downloads CORE B
88.	Towards the Use of Generative Adversarial Neural Networks to Attack Online Resources	Lelio Campanile, Mauro Iacono, Fabio Martinelli, Fiammetta Marulli, Michele Mastroianni, Francesco Mercaldo, Antonella Santone	Web, Artificial Intelligence and Network Applications	https://link.springer.com/chapter/10.1007/978-3-030-44038-1_81	Cited by 3 (Google Scholar, 12/21) 1.3k downloads CORE B
89.	Predicting Probability of Default Under IFRS 9 Through Data Mining Techniques	Fabio Martinelli, Francesco Mercaldo,	Web, Artificial Intelligence and	https://link.springer.com/chapter/10.1007/978-3-030-44038-1_87	Cited by 0 (Google Scholar, 12/21) 959 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
		Domenico Raucci, Antonella Santone	Network Applications		CORE B
90.	Code Reordering Obfuscation Technique Detection by Means of Weak Bisimulation	Giuseppe Crincoli, Tiziano Marinaro, Fabio Martinelli, Francesco Meraldo, Antonella Santone	International Conference on Advanced Information Networking and Applications (AINA- 2020)	https://link.springer.com/ chapter/10.1007/978-3- 030-44041-1_116	Cited by 3 (Google Scholar, 12/21) 1.4k downloads CORE B
91.	Android Run-time Permission Exploitation User Awareness by Means of Formal Methods	Fausto Fasano, Fabio Martinelli, Francesco Meraldo, Antonella Santone	International Conference on Information Systems Security and Privacy, ICISSP 2020	https://www.scitepress.or g/Link.aspx?doi=10.5220 /0009372308040814	Cited by 0 (Google Scholar, 12/21) NA downloads
92.	Accidental Sensitive Data Leaks Prevention via Formal Verification	Madalina G. Ciobanu, Fausto Fasano, Fabio Martinelli, Francesco Meraldo, Antonella Santone	International Conference on Information Systems Security and Privacy, ICISSP 2020	https://www.scitepress.or g/Link.aspx?doi=10.5220 /0009380608250834	Cited by 0 (Google Scholar, 12/21) NA downloads
93.	Bank Credit Risk Management based on Data Mining Techniques	Fabio Martinelli, Francesco Meraldo, Domenico Raucci, Antonella Santone	International Conference on Information Systems Security and Privacy, ICISSP 2020	https://www.scitepress.or g/Link.aspx?doi=10.5220 /0009371808370843	Cited by 0 (Google Scholar, 12/21) NA downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
94.	Malicious Collusion Detection in Mobile Environment by means of Model Checking	Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	International Joint Conference on Neural Networks, IJCNN 2020	https://ieeexplore.ieee.org/abstract/document/9207638	Cited by 5 (Google Scholar, 12/21) 46 downloads
95.	Enhanced Privacy and Data Protection using Natural Language Processing and Artificial Intelligence	Fabio Martinelli, Fiammetta Marulli, Francesco Mercaldo, Stefano Marrone, Antonella Santone	International Joint Conference on Neural Networks, IJCNN 2020	https://ieeexplore.ieee.org/document/9206801	Cited by 7 (Google Scholar, 12/21) 224 downloads CORE A
96.	Image-based Malware Family Detection: An Assessment between Feature Extraction and Classification Techniques	Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	IoT BDS 2020	https://www.scitepress.org/Link.aspx?doi=10.5220/0009817804990506	Cited by 7 (Google Scholar, 12/21) NA downloads
97.	Evaluating Deep Learning Classification Reliability in Android Malware Family Detection	Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo, Antonella Santone	2020 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)	DOI: 10.1109/ISSREW51248.2020.00082	Cited by 4 (Google Scholar, 12/21) 94 downloads
98.	A Deep-Learning-Based Framework for Supporting Analysis and Detection of Attacks on CAN Buses	Alfredo Cuzzocrea, Francesco Mercaldo, Fabio Martinelli	International Conference on Knowledge-Based and Intelligent Information & Engineering Systems KES 2020	https://doi.org/10.1016/j.procs.2020.09.203	Cited by 0 (Google Scholar, 12/21) NA downloads CORE B

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
99.	Machine Learning for Driver Detection through CAN bus	Fabio Martinelli, Francesco Mercaldo, Antonella Santone	2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)	DOI: 10.1109/VTC2020-Spring48590.2020.9129371	Cited by 4 (Google Scholar, 12/21) 139 downloads CORE B
100.	Information Sharing in Cyber Defence Exercises	Eduardas Kutka, Aušrius Juozapavičius, Linas Bukauskas, Agnė Brilingaitė	Proceedings of the 19th European Conference on Cyber Warfare and Security ECCWS 202	DOI: 10.34190/EWS.20.034	Cited by 1 (Google Scholar, 12/21) NA downloads
101.	Preprocessing Pipelines Including Block-Matching Convolutional Neural Network for Image Denoising to Robustify Deep Reidentification against Evasion Attacks	Marek Pawlicki Ryszard S. Choraś	JCR journal ENTROPY	https://doi.org/10.3390/e23101304	Cited by 0 (Google Scholar, 12/21) 219 downloads
102.	New explainability method for BERT-based model in fake news detection.	Szczepański, M., Pawlicki, M., Kozik, R. et al.	Sci Rep 11, 23705 (2021)	https://doi.org/10.1038/s41598-021-03100-6	
103.	Experimental analysis of the electromagnetic instruction skip fault model and consequences for software countermeasures	J.-M. Dutertre, A. Menu, O. Potin, J.- B. Rigaud, and J.- L. Danger	Microelectronics Reliability, 121, 2021.	https://doi.org/10.1016/j.microrel.2021.114133	Cited by 0 (Google Scholar, 12/21) 219 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
104.	Self-secured PUF: Protecting the Loop PUF by Masking	Tebelmann, L., Danger, J. L., & Pehl, M.	In <i>International Workshop on Constructive Side-Channel Analysis and Secure Design</i> (pp. 293-314). Springer, Cham.	https://hal.telecom-paris.fr/hal-03138858/document	Cited by 9 (Google Scholar, 12/21) 253 downloads
105.	Post-Quantum Era Privacy Protection for Intelligent Infrastructures	Lukas Malina, Petr Dzurenda, Sara Ricci, Jan Hajny, Gautam Srivastava, Raimundas Matulevičius, Abasi-amefon O. Affia, Maryline Laurent, Nazatul Sultan, Qiang Tang	IEEE	DOI: 10.1109/ACCESS.2021.3062201	Cited by 6 (Google Scholar, 12/21) 993 downloads
106.	Ensemble-Based Classification Using Neural Networks and Machine Learning Models for Windows PE Malware Detection	Damaševičius, Robertas; Venčkauskas, Algimantas; Toldinas, Jevgenijus; Grigaliūnas, Šarūnas	Electronics 10, no. 4: 485.	https://doi.org/10.3390/electronics10040485	Cited by 10 (Google Scholar, 12/21) 1780 downloads
107.	Securing Organization's Data: A Role-Based Authorized	Nazatul Haque Sultan, Maryline	IEEE Transactions on Cloud Computing	DOI: 10.1109/TCC.2021.3071304	Cited by 4 (Google Scholar, 12/21) 61 downloads

Nº	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	Keyword Search Scheme with Efficient Decryption	Laurent, Vijay Varadharajan			
108.	Development of the Information Security Management System Standard for Public Sector Organisations in Estonia	Mari Seeba, Raimundas Matulevicius, Ilmar Toom	24th International Conference on Business Information Systems - BIS 2021 conference	https://doi.org/10.52825/bis.v1i.43	Cited by 1 (Google Scholar, 12/21) NA downloads
109.	SI-AKAV: Secure integrated authentication and key agreement for cellular-connected IoT devices in vehicular social networks	Alireza Esfahani, Jérémie Decouchant, Marcus Völp, Shahid Mumtaz, Kostromitin Konstantin Igorevich	Transactions on Emerging Telecommunications Technologies Wiley Online Library	https://doi.org/10.1002/ett.4279	Cited by 0 (Google Scholar, 12/21) NA downloads
110.	CyberGSN: A Semi-formal Language for Specifying Safety Cases	Tewodros A. Beyene, Carmen Carlan	IEEE	DOI: 10.1109/DSN-W52860.2021.00021	Cited by 0 (Google Scholar, 12/21) 31 downloads
111.	Building Open Source Cyber Range To Teach Cyber Security	Tomas Lieskovan and Jan Hajný	ARES ETACS	https://doi.org/10.1145/3465481.3469188	Cited by 0 (Google Scholar, 12/21) 103 downloads
112.	Cybersecurity Curricula Designer	Jan Hajny, Sara Ricci, Edmundas Piesarskas and Marek Sikora	ARES ETACS	https://doi.org/10.1145/3465481.3469183	Cited by 0 (Google Scholar, 12/21) 34 downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
113.	Nautilus: A Tool For Automated Deployment And Sharing Of Cyber Range Scenarios	G. Bernardinetti, S. Iafrate and G. Bianchi	ARES 2021	https://doi.org/10.1145/3465481.3469182	Cited by 0 (Google Scholar, 12/21) 32 downloads
114.	Threat Modelling and Beyond - Novel Approaches to Cyber Secure the Smart Energy System	Heribert Vallant, Branka Stojanović, Josip Božić and Katharina Hofer-Schmitz	MDPI journal Applied Sciences	https://doi.org/10.3390/app11115149	Cited by 1 (Google Scholar, 12/21) 1079 downloads
115.	Risk-Oriented Design Approach For Forensic-Ready Software Systems	Lukas Daubner, Raimundas Matulevičius	ARES 2021	https://doi.org/10.1145/3465481.3470052	Cited by 0 (Google Scholar, 12/21) NA downloads
116.	Information Security Analysis in the Passenger-Autonomous Vehicle Interaction	Mariia Bakhtina, Raimundas Matulevičius	ARES 2021	https://doi.org/10.1145/3465481.3470045	Cited by 0 (Google Scholar, 12/21) 83 downloads
117.	Privacy-Preserving Online Parking Based on Smart Contracts	Petr Dzurenda, Carles Angles, Sara Ricci, Lukas Malina	ARES 2021	https://doi.org/10.1145/3465481.3470058	Cited by 0 (Google Scholar, 12/21) 33 downloads
118.	A Formal Analysis of EnOcean's Teach-in and Authentication	Katharina Hofer-Schmitz	ARES 2021	https://doi.org/10.1145/3465481.3470097	Cited by 1 (Google Scholar, 12/21) 22 downloads
119.	A Comparative Study of Automatic Software Repair Techniques for Security Vulnerabilities	Eduard Pinconschi, Rui Abreu, and Pedro Adão	The 32nd International Symposium on Software Reliability Engineering	Information not available yet	CORE A

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
			(ISSRE 2021) http://2021.issre.net/ Oct 25 - 28, 2021, Wuhan, China		
120.	A Novel Approach for Network Intrusion Detection Using Multistage Deep Learning Image Recognition	Toldinas, Jevgenijus, Algimantas Venčkauskas, Robertas Damaševičius, Šarūnas Grigaliūnas, Nerijus Morkevičius, and Edgaras Baranauskas	Electronics 10, no. 15: 1854.	https://doi.org/10.3390/electronics10151854	Cited by 1 (Google Scholar, 12/21) NA downloads
121.	VulnEx: Exploring Open-Source Software Vulnerabilities in Large Development Organizations to Understand Risk Exposure	Frederik L. Dennig, Eren Cakmak, Henrik Plate, Daniel A. Keim	IEEE Symposium on Visualization for Cyber Security 2021	https://arxiv.org/abs/2108.06259	Cited by 0 (Google Scholar, 12/21) NA downloads
122.	Security Risk Estimation and Management in Autonomous Driving Vehicles	Abasi-amefon O. Affia, Raimundas Matulevičius, and Rando Tõnisson	CAiSE 2021	https://doi.org/10.1007/978-3-030-79108-7_2	Cited by 0 (Google Scholar, 12/21) 583 downloads
123.	Hybroid: Toward Android Malware Detection and Categorization with	Mohammad Reza Norouzian, Peng Xu, Claudia	ISC 2021	https://www.sec.in.tum.de/i20/publications/hybroid-toward-android-malware-detectionand-	Cited by 0 (Google Scholar, 12/21) NA downloads

N°	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	Program Code and Network Traffic	Eckert, Apostolis Zarras		categorization-with-program-code-andnetwork-traffic	
124.	LastPyMile: Identifying the Discrepancy between Sources and Packages	Duc Ly Vu, Fabio Massacci, Ivan Pashchenko, Henrik Plate, Antonino Sabetta	ESEC/FSE 2021	https://doi.org/10.1145/3468264.3468592	Cited by 2 (Google Scholar, 12/21) NA downloads
125.	Analysis of a Laser-induced Instructions Replay Fault Model in a 32-bit Microcontroller	V. Khuat, J. -M. Dutertre and J. -L. Danger	<i>2021 24th Euromicro Conference on Digital System Design (DSD)</i> , 2021, pp. 363-370,	10.1109/DSD53832.2021.000061	Cited by 1 (Google Scholar, 12/21) 24 downloads
126.	Laser Fault Injection in a 32-bit Microcontroller: from the Flash Interface to the Execution Pipeline	V. Khuat, J. -L. Danger and J. -M. Dutertre	<i>2021 Workshop on Fault Detection and Tolerance in Cryptography (FDTC)</i> , 2021, pp. 74-85,	https://hal.archives-ouvertes.fr/hal-03433817/	Cited by 0 (Google Scholar, 12/21) 31 downloads
127.	Experimental analysis of the electro-magnetic instruction skip fault model and consequences for software countermeasures	J.-M. Dutertre, A. Menu, O. Potin, J.-B. Rigaud, and J.-L. Danger,	Microelectronics Reliability, 121, 2021.	https://doi.org/10.1016/j.microrel.2021.114133	Cited by 0 (Google Scholar, 12/21) NA downloads
128.	Multiple and Reproducible Fault Models on Micro-	V. Khuat, O. Trabelsi, L.	IEEE	10.1109/EMC/SI/PI/EMCEurope52599.2021.9559288	Cited by 2 (Google Scholar, 12/21) 13 downloads

Nº	Title	Authors/Owners	Journal/ Conference	DOI (publisher)	Number of citations, downloads and CORE ranking
	Controller using Electromagnetic Fault Injection	Sauvage, J-L. Danger.			
129.	A Large-Scale Analysis of IoT Firmware Version Distribution in the Wild	F. Ebbers,	IEEE Transactions on Software Engineering	10.1109/TSE.2022.3163 969	Cited by 1 (Google Scholar, 12/21) NA downloads
130.	Optimized Parameter Search Approach for Weight Modification Attack Targeting Deep Learning Models	Echeberria-Barrio, Xabier, Amaia Gil- Lerchundi, Raul Orduna-Urrutia, and Iñigo Mendialdua.	<i>Applied Sciences</i> 12, no. 8: 3725.	https://doi.org/10.3390/a pp12083725	N/A
131.	Understanding deep learning defences against adversarial examples through visualizations for dynamic risk assessment.	Echeberria-Barrio, X., Gil-Lerchundi A., Egana-Zubia, J. <i>et al.</i>	<i>Neural Comput & Applic</i> (2022).	https://doi.org/10.1007/s 00521-021-06812-y	N/A
132.	A Comparative Study of Automatic Program Repair Techniques for Security Vulnerabilities	Eduard Pinconschi; Rui Abreu; Pedro Adão	<i>IEEE</i>	10.1109/ISSRE52982.20 21.00031	N/A

Table 5: Final List of SPARTA Scientific publications

3.3 Monthly SPARTA workshops

The SPARTA monthly workshops seek to gather a diverse set of actors to get involved in the project and to build knowledge. WP12 supported the dissemination and communication of these workshops whenever possible, organized within the scope of WP3 and WP8, through publications on SPARTA's social media accounts and on the website. In total, there were 40 monthly workshops organized.

3.4 Campaigns for Diversity in Cybersecurity

SPARTA consortium was committed to understand and work towards the gender and diversity gap issue in cybersecurity as there is a collective consciousness that this is a social responsibility of public interest. As to reduce the gender gap and lack of human resources for cybersecurity in Europe, SPARTA has been addressing this issue by embedding several positive actions, described and summarized as follows.

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 was prepared to promote awareness of the current situation, ultimately aiming to attract women to the field. The activities designed and implemented in the scope of task 12.4 were in line with the communication and dissemination strategic objectives established in deliverable 12.1, and are reported and evaluated in deliverable 12.6.

The efforts made in the first year of the project targeted at promoting awareness on the cybersecurity gender and diversity gap issue and informing SPARTA target groups about the project position regarding it. Activities ranged from the Women's Day campaign, engagement with ECSO's "women4cyber" initiative, SPARTA presence at related events (womENCourage 2019) and SPARTA communication on the subject at cybersecurity events (LeHack 2019).

The second year called for the establishment of the "participation" axis and the activities mainly targeted at involving women in the cybersecurity field with the SPARTA project and collecting their inputs to understand the social barriers and roadblocks encountered when working on cybersecurity. This was achieved through the *Women in SPARTA* campaign, which allowed for sharing ideas, experiences and knowledge on the topic. These inputs were collected and analysed to create and deliver, during the third year of the project, the Best-practices Guide to Attract and Retain Women in Cybersecurity Teams. Other actions as the "Gender and Diversity Breakfast Webinars" also contributed to the participation axis.

The last year foresaw the deployment of the action axis, aimed at influencing practices. As such, WP12 built its activities with the ultimate goal of promoting changes in behaviour and practices, namely by introducing the cybersecurity reality and the gender gap in the field to high-school students through the event "SPARTA: The Future needs you!".

3.4.2 Outermost Regions Engagement

Task 12.5 *Outermost Regions engagement - 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 located in different geographies (Indian Ocean; the Atlantic Ocean and the Caribbean). Each living lab action targeted at 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 receiver's specific cybersecurity needs.

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 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 for achieving 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, whos' interest in the subject was keen.

Action 2 – Stimulate cybersecurity studies or training at the university level – aimed at providing the necessary means for the creation of a cybersecurity curriculum, ensuring that students at the university level have access to education on cybersecurity, a subject of growing critical importance. Overall, this action achieved its main goal as the University of Las Palmas de Gran Canaria showed a keen interest in establishing a Cybersecurity bachelor degree, in a collaborative effort with SPARTA, 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](#). This action can, in the future, be replicated in different European locations and beyond, as it had proven to be efficient and received positive feedback from ULPGC.

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 the will to promote cybersecurity actions. The resources and efforts of this action were maximised by the creation of a second on-site workshop with SMEs on the digital sector from La Reunion, expanding the reach and impact of the SPARTA project.

Chapter 4 Communication and Dissemination

Instruments

Chapter 4 considers the C&D instruments that have been updated during the third year of the project to improve their efficiency, ensuring that the project's communication objectives have a cohesive instrumental base to be addressed.

4.1 SPARTA Official Website

The SPARTA [website](#) has been often updated and worked on during the whole project lifetime, in collaborative work between all WPs, led by INOV and CEA, to ensure SPARTA delivers a dynamic, intuitive, and complete platform to its visitors:

- The main page of the website welcomes the visitors with the latest “Events” and “News”, separately;
- The website provides information about SPARTA, SPARTA’ challenges, structure, and partners on a single page;
- The “Results” page features all the SPARTA publications, deliverables, podcasts, and demonstrators;
- The scientific publications are stored and organised to facilitate the search process, allowing for more acute dissemination of these contents. Through this page link, one can share the papers on SPARTA social media platforms (LinkedIn and Twitter).
- The website has a dedicated section for the Training and Awareness WP9;
- It also has a dedicated page to the Gender and Diversity dimension of SARTA;
- The JCCI is part of the SPARTA website and is leveraged through several publications on social media.

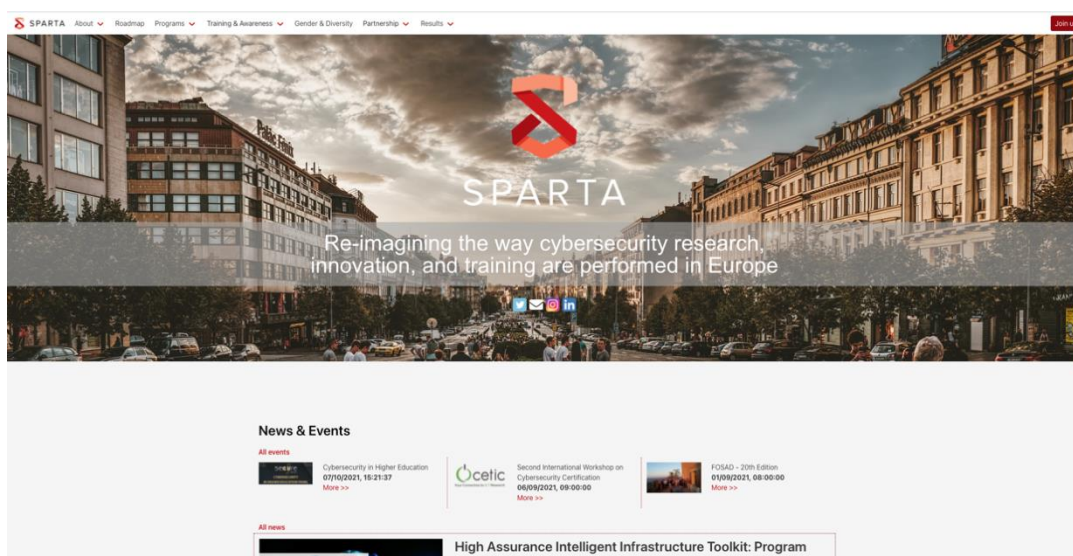
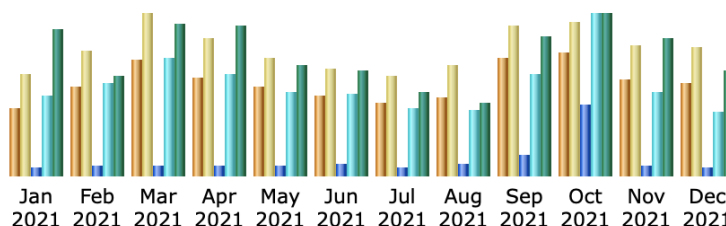


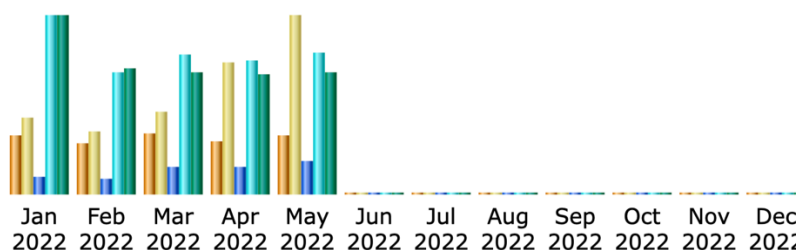
Figure 2: SPARTA Website front page

Partners contributions to ensuring diversity, periodicity and relevance of publications on the SPARTA website resulted in a steady number of unique visitors per month. Here we present the number of visitors from January 2021 to December 2021, and the numbers of visitors during the extension of the SPARTA project, from January 2022 to May 2022.



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2021	1,549	2,320	5,628	51,096	30.37 GB
Feb 2021	2,021	2,838	5,867	58,258	20.56 GB
Mar 2021	2,625	3,691	6,777	74,184	31.61 GB
Apr 2021	2,223	3,135	6,699	64,031	31.36 GB
May 2021	2,046	2,679	6,777	53,467	22.92 GB
Jun 2021	1,835	2,433	7,459	52,314	21.88 GB
Jul 2021	1,652	2,260	5,341	42,416	17.22 GB
Aug 2021	1,778	2,515	7,634	41,101	15.02 GB
Sep 2021	2,671	3,422	12,989	64,437	28.77 GB
Oct 2021	2,800	3,518	44,992	102,539	33.61 GB
Nov 2021	2,192	2,992	6,552	53,219	28.57 GB
Dec 2021	2,128	2,936	5,099	40,399	21.92 GB
Total	25,520	34,739	121,814	697,461	303.81 GB

Figure 3: 2021 Monthly History of Visitors to the Website



Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2022	1,908	2,545	5,591	57,472	28.37 GB
Feb 2022	1,642	2,090	5,007	39,033	20.07 GB
Mar 2022	2,016	2,721	8,760	44,717	19.26 GB
Apr 2022	1,763	4,329	8,341	43,157	19.00 GB
May 2022	1,940	5,888	10,389	45,508	19.35 GB
Total	9,269	17,573	38,088	229,887	106.05 GB

Figure 4: 2022 Monthly History of Visitors to the Website

4.2 SPARTA social media

Deliverable 12.4 established the need for communicating the SPARTA results through **advertisements** as they are proven to effectively and efficiently deliver messages to targeted audiences and assure the outreach of publications to many people. As such, during the third year of the project, some content was promoted on Twitter, which led to a growing number of

followers and a bigger reach of the SPARTA results to our target audiences. Twitter was the selected social media platform to perform these advertisements because of its proximity to all our target audiences and suitability for the cybersecurity community. The C&D team selected the messages related to the main results of the SPARTA project and events to advertise on social media accounts.

Hootsuite, a social media content management tool, coordinates and manages all publications efficiently, allowing for streamlined teamwork to organize, schedule, and publish content effortlessly to all SPARTA social media accounts.

The C&D strategy adopted for the SPARTA social media accounts and the updates established in deliverables 12.3 and 12.4 have contributed to the project's visibility and the engagement of target groups with the SPARTA values, goals, activities and results. It helped achieve 1371 followers on Twitter, 674 on LinkedIn, and 252 on Instagram, and create a SPARTA community.

4.2.1 LinkedIn

During the third year of the project, the SPARTA LinkedIn page received, on average, 80 visitors each month, through the mobile and desktop – Figure 5. During the extension period, there was a higher number of visitors (around 250) in April due to the *Hack Me, I'm Famous* event – Figure 6. SPARTA audience was generally interested in STEM areas, with a major incidence on Informational Technology, Business Development and research. The majority of visitors were from different industries, such as Research Information Technology and Services, Computer and Network Security and Higher Education and Defense – Figure 7. Overall, the project was able to build a diverse community in the social media networks, from different backgrounds and domains of knowledge.

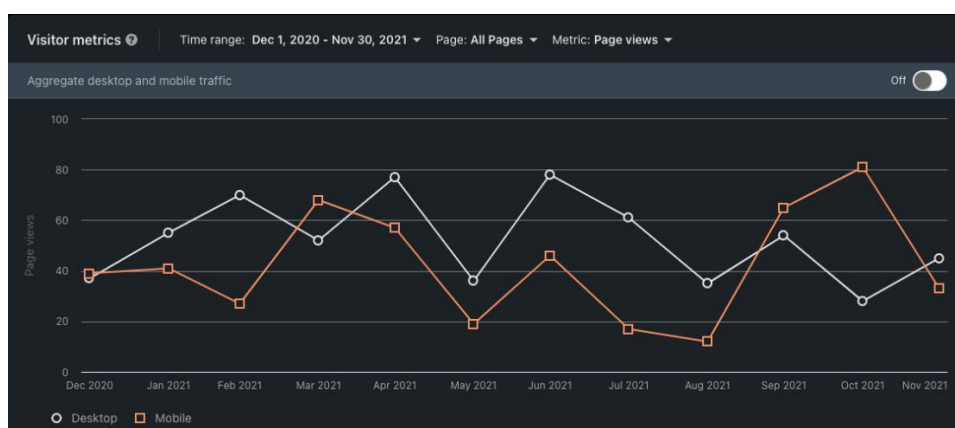


Figure 5: LinkedIn visitor metrics 2020-2021

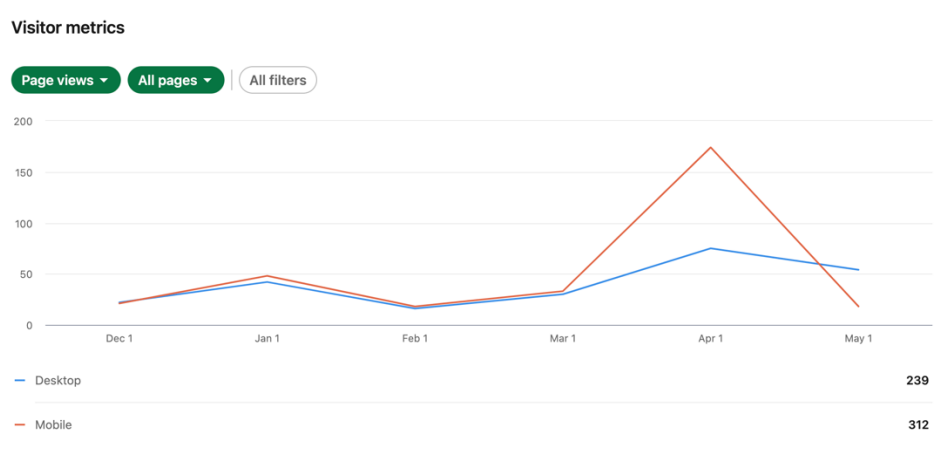


Figure 6: LinkedIn visitor metrics 2022

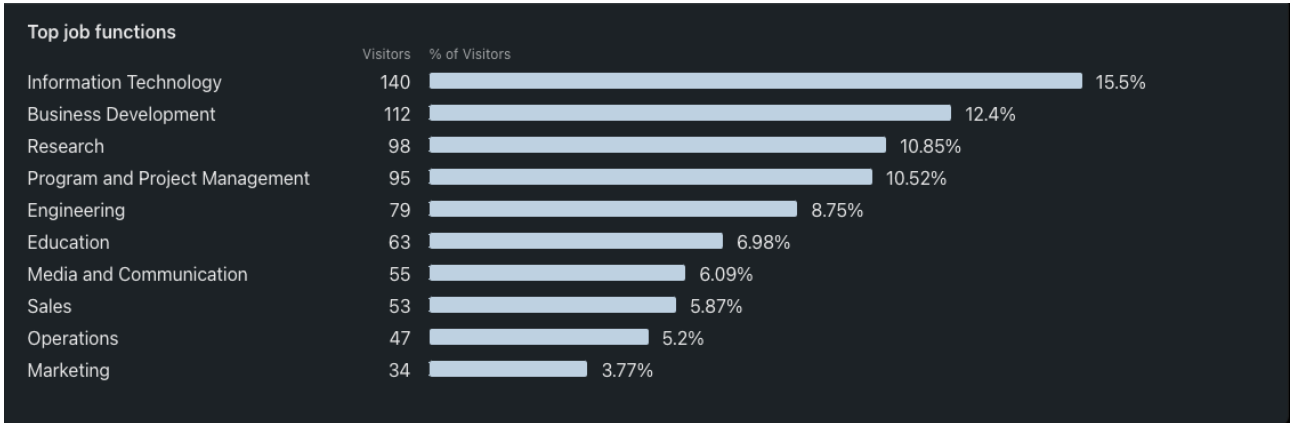


Figure 7: LinkedIn visitor demographics (top job functions 2020-2022)

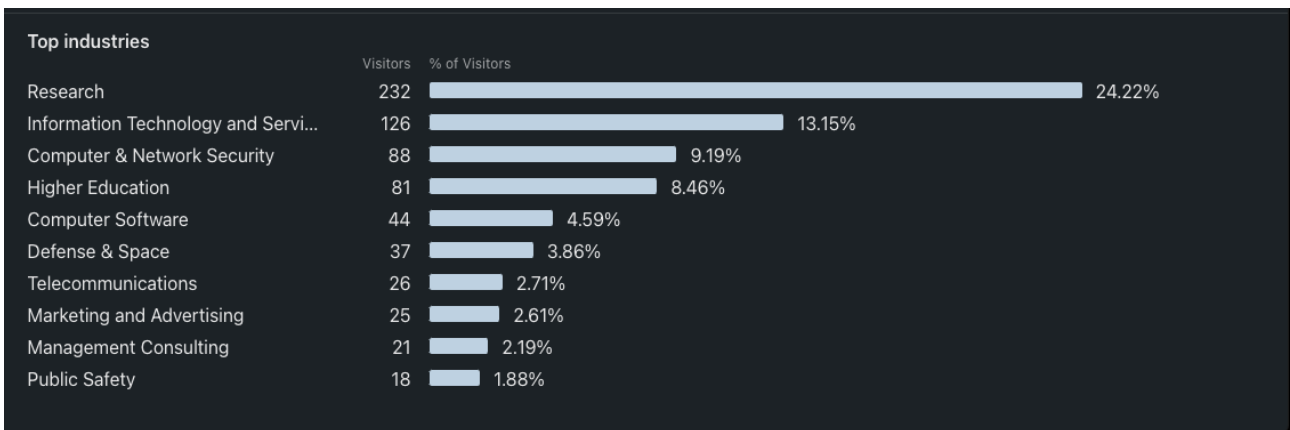


Figure 8: LinkedIn visitor demographics (top industries 2022)

4.2.2 Instagram

Instagram is the SPARTA main platform to reach a younger and more diverse audience. Deliverable 12.4 established the need for addressing the gender gap in the audience as at the time we had 66% of male followers. Through a strategy adopted to engage and attract more female audiences, the gender gap shortened – Figure 9 – where 55% are men and 44,9% are women. Followers’ ages range between 18 and 54 years old. Instagram privileges the use of images and videos over long texts. It was the main platform for sharing instant contents using the “stories” tool, which allows for covering events live, sharing contents from other relevant accounts (@digitaleu; @ECOSO; @europeancommision; etc.) The platform is not advisable if the goal is to reach the cybersecurity

community. Instagram can be an efficient tool to communicate with not specialized communities and younger audiences.

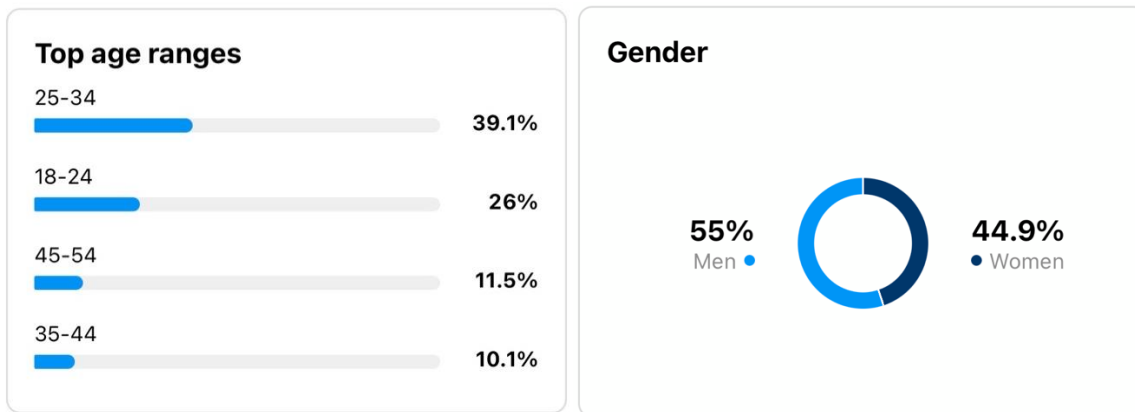


Figure 9: Age and gender of SPARTA Audience on Instagram

4.2.3 Twitter

The audience analytics information is not available as Twitter has removed this option since the end of January 2020 (Hutchinson, 2020) - making it impossible to evaluate both the SPARTA audience features and the gender gap. Annexe 1 summarizes SPARTA activities on the Twitter social media network. Twitter is the most efficient platform to communicate and disseminate European Projects as SPARTA. The Cybersecurity community and the overall EU funded project community and interested people are on Twitter.

4.3 Contribution of partner to C&D activities

The strategy deployed on the D12.3 to maximize partners' contribution through their direct participation in the production of content to be shared on SPARTA social media accounts and the website has shown to be efficient, keeping the audiences updated and informed about several aspects related to the SPARTA project and cybersecurity field. This strategy endured until the end of the project and guided the contribution of partners to communication and dissemination activities.

During the second and third years of the project, and although the COVID-19 has had a great impact on all the activities planned, partners conducted several activities to promote awareness of and involvement in the SPARTA project, namely through the participation in and organisation of diverse events. Through the entire duration of the project, partners were keen to help building a strong and coherent communication of the project, accordingly to what was proposed in D.12.1.

4.4 Media Relations

During the period M24 – M41, the SPARTA project continued to have some presence on other media platforms. The C&D team has been interacting with the editor of the EU's Cybersecurity & Digital Privacy Newsletter to promote regular publications about the project in this newsletter. Table 3 highlights some of SPARTA presence in the media relative to the third year of the project, with the respective links to publication:

<p>Journal of Information Security and Applications Volume 61, September 2021, 102916</p> <p>Stakeholder perspectives and requirements on cybersecurity in Europe</p> <p>Simone Fischer-Hübner^{a, R}, Cristina Alcaraz^a, Afonso Ferreira^a, Carmen Fernandez-Gago^b, Javier Lopez^b, Evangelos Markatos^c, Lejla Islami^d, Mahdi Akil^d</p> <p>https://doi.org/10.1016/j.jisa.2021.102916</p>	<p>GO CYBER WITH SPARTA</p> <p>5 Novembro 9H00 - 12H00</p> <p>Colégio dos Jesuítas, Patto I</p> <p>PROGRAMA</p> <ul style="list-style-type: none"> Sessão de boas-vindas (9H00) Apresentação do projeto SPARTA Programa de Ações Coffee break Aspectos humanos da cibersegurança - Engenharia Social Gestão e Análise de Risco
<p>CYBERSECURITY COMPETENCE CENTRE PILOT PROJECTS SME Impact and Opportunities</p> <p>Workshop 14 July 2021 09.00-11.00 CEST</p>	<p>SCIENCE BUSINESS[®] Bringing together industry, research and policy</p> <p>Europe looks to raise its game in cybersecurity</p> <p>18 Mar 2021 </p> <p>Replacing a fragmented network of players with an EU digital sovereignty ecosystem</p>
<p>SPARTA DAY & BROKERAGE EVENT: WE ARE CONNECTED</p> <p>12 April 2021 6 views 1 min read</p> <p>SWForum.eu / All Events / SPARTA DAY & BROKERAGE EV...</p>	<p>SPARTA</p> <p>During this year's SECURE conference we invite you to a special track dedicated to the SPARTA project.</p> <p>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 set up unique catalyst leading the way in building transformative capabilities and forming a world-leading Cybersecurity Competence Network across the EU. From basic human needs (their activities (energy, finance, and transport) to technologies (ICT and industry) to sovereignty (eGovernment, public administration), four research and innovation programs</p>
<p>SPARTA-Video from Demo in Work Package 6</p> <p>Secure Orchestration - Modeling, Verification and Testing</p>	<p>SPARTA – CAPE Secure Consumption of Open Source</p> <p>This demo presents a series of tools aiming at evaluating the security of the open-source software supply chain. More specifically...</p>
<p>Women in SPARTA – Luana Fabrete</p> <p>Luana Fabrete, an industrial engineer from Technikon briefly speaks about her experiences as a woman in the tech field. Currently...</p>	<p>Women in SPARTA – Aleksandra Pawlicka</p> <p>SPARTA has been researching the issues that may be at the backbone of the gender gap faced in the cybersecurity...</p>

Table 6: SPARTA presence on media platforms

4.5 Podcasts

The five podcasts launched by Technikon are available on the dedicated SPARTA website page: <https://sparta.eu/podcasts/>, and are being disseminated on SPARTA social media networks.

- Ep.1: What is SPARTA?
- Ep.2: European government and private businesses preparedness for cyber-attacks
- Ep.3: Responsible Innovation
- Ep.4: Reforming Cybersecurity in the EU through SPARTA project
- Ep.5: Everyone Matters
- Ep.6: Special series: An Insider's View of Where Cybersecurity Meets Pandemic

A three-podcast series entitled "Where Pandemic Meets Cybersecurity" was launched during the outbreak of the COVID-19 pandemic to address how the pandemic impacted partners work and what similarities exist between global pandemics and cyber-attacks. This podcast series was [acknowledged](#) at CORDIS and had a good outreach on social media and education. The Greek magazine Koutipandoras has also [published](#) news related to this podcast series.

4.6 Videos

During the third year of the project, INOV produced teasers to introduce the SPARTA results on social media. The following links provide a few examples:

- https://twitter.com/sparta_eu/status/1451531731585142784/video/1
- https://twitter.com/sparta_eu/status/1446238658181337093/video/1
- https://twitter.com/sparta_eu/status/1420083242535989251/video/1
- https://twitter.com/sparta_eu/status/1418528849579683841/video/1

Other videos are the interviews made in the Women in SPARTA campaign context, published on several platforms as described in deliverable 12.6. In addition, further videos were produced by Technikon, which can be found on the project website and social media. As acknowledged in deliverables 12.3 and 12.4, videos have shown to be publications on social media with higher engagement rates.

4.7 Demonstrators

Partners have produced several demonstrators to present the SPARTA results, all stored in the SPARTA official website - <https://sparta.eu/papers/#demos>. These demonstrators have also been published on the SPARTA social media accounts and the monthly *SPARTA NEWS*, ensuring the dissemination of results to our target audiences:

1. LastPyMile: Identifying the Discrepancy between Sources and Packages
2. SPARTA HAIL-T: Secure Orchestration - Modeling, Verification and Testing
3. SPARTA: Demonstrator Connected Car Basic Scenario (CACC Platoon)
4. Foreshadow-VMM: Feasibility and Network Perspective
5. Digital Literacy and Cybersecurity Awareness During the COVID-19 pandemic
6. A Method for Managing GDPR Compliance in Business Processes

Demonstrators, like videos, have shown to be an efficient format to deliver the messages related to the SPARTA results.

4.8 Internal Communication Instruments

Deliverable 12.4 updated the strategy defined in deliverable 12.3 to be implemented during the third year of the project, which aimed at building a cohesive internal communication flow. As a result, the internal bi-monthly newsletter and the use of the *Stackfield* tool to promote easier collaboration among partners were ceased as they proved to be inefficient and unpopular among partners. The evaluation of these tools can be found in deliverable 12.4.

4.8.1 SPARTA NEWS

Instead of the internal bi-monthly newsletter – described in detail in deliverables 12.3 and 12.4 –, the C&D team started to deliver the news published on the SPARTA website and other internal news to the partners through a dedicated e-mail sent to the SPARTA internal mailing list

– project.consortium@internal.sparta.eu – as well as to the project associates associates@sparta.eu – and friends – friends@sparta.eu. The adoption of this strategy lied in the simplification of the process, avoiding dependency on timely-delivered contents, and has proven to be efficient as there was positive feedback about this new format.

4.8.2 NextCloud

During the third year of the project, *NextCloud* was the main and official platform used to facilitate and promote collaborations, store and share documents and ease communications between partners. It has proven to be an efficient tool and overall partners adhere to the platform, using it daily. Partners could have made a faster transition from SVN and *stackfield* to NextCloud if the tool had been introduced to the consortium at the very beginning of the year. As it was introduced in a more phased approach, it took more time for partners to fully engage with and use the platform.

4.9 Review Recommendations

WP12 considered the recommendations made during the M18 review, and the C&D team adopted measures to ensure that all activities are targeted at creating impact and promoting reach with publicity, along with the correct report on both outcomes/impact and outputs/activities. WP12 established a publishing calendar that relied on inputs from the WPs related to their work and achievements. WP12 collects the analytics from the platforms to monitor the reach of such publications, which are reported on this deliverable, as well as the type of community that we were able to build. Deliverables 12.6 *Closing the Gender and Diversity Gap* and 12.7 *Outermost Regions Engagement* also report the impact of the activities conducted to promote diversity and ensure inclusion in cybersecurity. Nonetheless, the communication flow between SPARTA partners could have profited from on-site meetings if not the pandemic. On-site meetings continue to lead the tools for collaborations.

Chapter 5 Third-year general evaluation

During the third year of the project and its extension, SPARTA nurtured and maintained the “awareness” and “participation” axes, and strived to leverage the “action” axis, targeting the communication and dissemination efforts at changing attitudinal behaviour, that is of public interest, towards cybersecurity actions such as the 1) adoption of cybersecurity habits; 2) the acquisition from the industries of cybersecurity services, and the 3) academy starting to direct their interests and activities towards the issue.

The “awareness” and “participation” axes were nourished through a coherent publishing calendar – to keep SPARTA audiences engaged and aware of the project aims, values, activities and (during the third year) monthly results –, interactions with other media platforms such as the Cybersecurity and Digital Privacy Newsletter, organization of the SPARTA monthly workshops, participation on several events, and publishing scientific papers and demonstrators.

As countries and partners started to gain resilience towards the COVID-19 pandemic impacts on the implementation of planned C&D activities, the achievement of the objectives set in deliverables 12.1, 12.3 and 12.4 became possible. Activities were re-designed or re-scheduled and implemented as we learned how to deal with the pandemic impacts and constraints, avoiding compromising the SPARTA expected results.

The diversity of actors inherent to the SPARTA project has shown, once more, that it enhances the possibility of outreach to a broader set of audiences across geographies, only this time online.

The use of platforms for online meetings and social media networks have shown to be efficient tools to replace face-to-face meetings, events, and communication materials. Nonetheless, the communication flow between the SPARTA partners, associates and friends – enhanced by the monthly SPARTA NEWS and the use of NextCloud – would have profit from on-site meetings, such as the SPARTA days.

The “action” axis was also leveraged by these actions, but mostly through the Monthly SPARTA workshops, the WP9 activities and the deployment of the *Go cyber with SPARTA (task 12.5)* campaign, established through several on-site and online workshops that influenced academy, critical infrastructure and several SMEs changing attitudinal behaviour towards cybersecurity. The event “SPARTA: The Future Needs you” equally contributed to these objectives.

The gender and diversity dimension of the project has been enhanced during this period, allowing for more incisive actions and collaborations. The gender gap of SPARTA social media accounts, namely on Instagram, as well as at the SPARTA events has dropped.

Chapter 6 Summary and Conclusion

As a result of the evaluation made to the activities developed during the third year of the project, as well as the reports and evaluations made in the previous deliverables, chapter 6 seeks to provide a brief summary of the main lessons learned during the three years of the SPARTA project.

The selection and definition of communication and dissemination strategic axes, aligned with the project's main objectives, has shown to be efficient for targeting efforts and maximizing resources. The three interdependent strategic axes established for the SPARTA project were essential in guiding activities and for achieving the main communication and dissemination goals, in line with the overall project's objectives.

- **Internal Communication:**

Managing the communication and dissemination activities of a 44 partners consortium across geographies requires the use of collaborative tools and their correct and timely introduction to avoid scattering and lack of use.

The COVID-19 pandemic restrictions have shown that almost all types of collaboration and events are possible through online platforms, thus giving a prospect of different ways partners can reduce their carbon footprint for meetings and workshops. Nonetheless, the on-site events are the privileged platform for building strong collaborations and commitments. The swift transition to online platforms had an impact on the communication flow between partners, making it difficult for building trust and set collaboration avenues.

The deployment of the monthly SPARTA News contributed to keeping partners, associates and friends aware of all the projects activities and results. Their contribution to the creation of content sharpened their engagement with the project.

- **Outside Communication:**

The website, as well as the SPARTA social media accounts, are the main interfaces that link the project to its audiences. It is the tools that allow to engage the community with the project's objectives, values, activities and results. The collaborative efforts of WP1 and WP12 with all the project's partners were essential to delivering relevant and updated information about the project. The website was continuously under major changes to ensure that visitors always found updated and relevant information on the project and to facilitate the storage and sharing of public information.

The social media accounts, like the website, were continuously nourished by coherent and constant publications about SPARTA aims, values, activities and results. The contribution of all partners was, once again, the basis to keep audiences informed and engaged with the project. Using advertisements may be advisable to have a bigger reach between the selected targeted groups. They are proven to effectively and efficiently deliver messages to targeted audiences and assure the outreach of publications to many people. It may also be advisable to use a social media content management tool (such as Hootsuite) to coordinate and manage all publications efficiently, allowing for streamlined teamwork to organize, schedule, and publish content effortlessly to all social media accounts.

These networks have been important to ensure SPARTA visibility, communicate the project's main messages, foster conversations, and raise awareness on cybersecurity and its challenges. Since the restrictions imposed by the COVID19 pandemic, such as to cease all the grand events, social media networks have served as the primary channel to keep audiences engaged with the project. On-site events are a privileged means for promoting awareness and action towards a specific objective. SPARTA was able to organize and participate in several conferences, events and workshops that allowed the project for building a diverse community and promote cybersecurity awareness and behaviour. Other communication and dissemination materials such as podcasts, videos, and demonstrators have equally shown to be efficient in delivering specific and detailed messages.

- **Gender and Diversity**

SPARTA consortium was committed to understanding and working towards the gender and diversity gap issue in cybersecurity as there is a common realization that this is a social responsibility of public interest. Deliverables 12.6. *Closing the Gender Gap* and D12.7 *Outermost Regions Engagement – “Go Cyber with SPARTA” campaign* report and evaluates the activities developed in this scope.

List of Abbreviations

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


Annex 1 – Twitter Analytics

Jan 2021 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 1,445 impressions
 SPARTA wishes you a secure and happy new year 2021!
 We leave you with some reading and future perspectives for #Europe #CyberSecurity : ec.europa.eu/digital-single...

@DSMeu @EU_Commission @Cybersec_EU @ecso_eu @CCN_EU @ECHOcybersec @CyberSec4Europe @concordiah2020 pic.twitter.com/kqx0Gnavz




11 retweets 20 likes

[View all Tweet activity](#)

[View Tweet activity](#)

Top Follower followed by 2,882 people



5GCity @5GCity **FOLLOWS YOU**
 This project receives funding from the [EU H2020](#) Research & Innovation Programme.
[View profile](#)


JAN 2021 SUMMARY

Tweets	4	Tweet impressions	6,979
Profile visits	383	Mentions	6
New followers	26		

Top mention earned 33 engagements
 Don't miss the article on "Threat analysis and model developed in @sparta_eu SAFAIR Program". Discover the four AI attack tactic groups identified!
ow.ly/JVDQ50Dly6q

#horizon2020 #cybersecurity #threatanalysis

@Vicomech @EU_Commission @CCN_EU @Cybersec_EU pic.twitter.com/ttYE34mPe




5 retweets 11 likes

[View all Tweet activity](#)

[View Tweet activity](#)

Top media Tweet earned 629 impressions
 SAVE THE DATE for another SPARTA workshop on 29th January, 12:00 CET, this time about the #Cybersecurity Landscape in #Greece 🇬🇷 The workshop is enriched with an interdisciplinary panel of speakers and interesting conversations!
 Register here ec.europa.eu/eusurvey/runne...
pic.twitter.com/4qj5VnBP6



6 retweets 13 likes

[View all Tweet activity](#)

[View Tweet activity](#)

Feb 2021 • 28 days

TWEET HIGHLIGHTS

Top Tweet earned 1,905 impressions
 @sparta.eu and @concordiah2020 joined forces to build an #ecosystem of institutions that provide unique technical resources to partners and cooperate on the organization of #trainings 🙌🌍👏

Learn more link.in/e3FYnE
[#cybersecurity #KYPO #CCN](https://twitter.com/5LgAoOogty)
pic.twitter.com/5LgAoOogty



🔗 1 🗨️ 12 ❤️ 13

[View all Tweet activity](#)

[View Tweet activity](#)

Top mention earned 58 engagements



Dr Michael Cooke 🇮🇪 🇫🇷 🇵🇹 🇬🇧
 @MichaelCooke76 · Feb 22
 Funded #SFI @scienceirel PhD opportunity on Psychology of #CyberSecurity with @deirdre_desmond and me. @AdvanceCrt @ECHOcybersec @Cybersec_EU @BPSCyberPsych @sparta.eu @CyberSecOb @MaynoothUni advance-crt.ie/apply/

🔗 1 🗨️ 1 ❤️ 7

[View Tweet](#)

Top media Tweet earned 1,749 impressions

👤 DataBreach: The Good, the bad and the Ugly 🤖 What can we learn from #cyber #criminals? #Leaks have become a significant market and business opportunity 🌐

Learn more sparta.eu/news/2021-01-1-...
pic.twitter.com/8Rd9DsaldB



🔗 7 ❤️ 13

[View all Tweet activity](#)

[View Tweet activity](#)

FEB 2021 SUMMARY

Tweets	11	Tweet impressions	15.2K
Profile visits	484	Mentions	17
New followers	14		

Mar 2021 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 6,248 impressions
 🙌 Why does the industry fail to attract and retain #women in #CyberSecurity ? @sparta.eu launched a guide to help companies understand the reasons why and to promote a more #inclusive, #diverse and #attractive workplace.

sparta.eu/news/2021-03-0-...
pic.twitter.com/fThlMenalc



🔗 2 🗨️ 56 ❤️ 960

[View all Tweet activity](#)

[View Tweet activity](#)

Top mention earned 1,194 engagements
 🙌 Why does the industry fail to attract and retain #women in #CyberSecurity ? @sparta.eu launched a guide to help companies understand the reasons why and to promote a more #inclusive, #diverse and #attractive workplace.

sparta.eu/news/2021-03-0-...
pic.twitter.com/fThlMenalc



🔗 2 🗨️ 56 ❤️ 960

[View all Tweet activity](#)

[View Tweet activity](#)

Top Follower followed by 6,187 people



NASK
 @NASK_pl [FOLLOWS YOU](#)

[View profile](#)

Top media Tweet earned 3,788 impressions

Ready to play? The @sparta.eu SAFAIR AI contest is launched! It aims to evaluate the robustness of a #defence technique by means of a two-player game. You can either play in the Attack or Defence tracks.

Learn more sparta.eu/news/2021-03-0-...

[#DeepLearning](#)
 @TU_Muenchen
pic.twitter.com/OYGBqimXit



🔗 7 ❤️ 7

[View all Tweet activity](#)

[View Tweet activity](#)

MAR 2021 SUMMARY

Tweets	8	Tweet impressions	132K
Profile visits	2,604	Mentions	30
New followers	18		

Apr 2021 · 30 days

TWEET HIGHLIGHTS

Top Tweet earned 2,866 impressions

The SPARTA Brokerage event is now taking place 🎉

[#partnership #cybersecurity](#)
<pic.twitter.com/dN2DFISebY>


🔄 7 ❤️ 11

[View all Tweet activity](#)
[View Tweet activity](#)
Top Follower followed by 2,660 people

Vojvodina ICT cluster
 @VOICT · FOLLOWS YOU

Single point of contact with the best #ICT companies in #Serbia.

[View profile](#)
Top mention earned 101 engagements

CyberSec_EU

@Cybersec_EU · Apr 16

Building up the #EU #Cybersecurity Competence Centre: today we hosted the first Informal Governing Board.

 Learn more ➡ europa.eu/fgC77nK
[@DigitalEU](#) [@REA_research](#) [@enisa_eu](#)
[@concordiah2020](#) [@sparta_eu](#) [@ecso_eu](#)
[@ECHOcybersec](#) [@cinea_eu](#)
[@CyberSec4Europe](#) [@cyberwatchingeu](#)
twitter.com/LorenaBoix/sta...

🔄 21 ❤️ 30

[View Tweet](#)
Top media Tweet earned 1,577

impressions

[@sparta_eu](#) Training and Awareness team launched the Curricula Designer, a simple free web-based application that helps education and training providers to design #cybersecurity curricula that reflect needs of current job market 🎓 👤 🔧

 Learn more ➡ sparta.eu/news/2021-04-0...
<pic.twitter.com/GliifWnXpaD>


🔄 9 ❤️ 8

[View all Tweet activity](#)
[View Tweet activity](#)

APR 2021 SUMMARY

Tweets	17	Tweet impressions	19.3K
Profile visits	1,357	Mentions	22
New followers	31		

Jan 2021 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 1,445 impressions
 SPARTA wishes you a secure and happy new year 2021!
 We leave you with some reading and future perspectives for #Europe #CyberSecurity :
ec.europa.eu/digital-single...

@DSMeu @EU_Commission
 @Cybersec_EU @ecso_eu @CCN_EU
 @ECHOcybersec @CyberSec4Europe
 @concordiah2020
pic.twitter.com/lkpxoGnavz



11 retweets 20 likes

[View all Tweet activity](#)

[View Tweet activity](#)

Top Follower followed by 2,882 people



5GCity
 @5GCity **FOLLOWS YOU**
 This project receives funding from the
EU_H2020 Research & Innovation
 Programme.

[View profile](#)

Top mention earned 33 engagements
 Don't miss the article on "Threat analysis and model developed in @sparta_eu SAFAIR Program". Discover the four AI attack tactic groups identified!

ow.ly/JVDO50Dly6q

#horizon2020 #cybersecurity #threatanalysis

@Vicomech @EU_Commission
 @CCN_EU @Cybersec_EU
pic.twitter.com/ttYEM4mPe



5 retweets 11 likes

[View all Tweet activity](#)

[View Tweet activity](#)

Top media Tweet earned 629 impressions

SAVE THE DATE for another SPARTA workshop on 29th January, 12:00 CET, this time about the #Cybersecurity Landscape in #Greece 🇬🇷 The workshop is enriched with an interdisciplinary panel of speakers and interesting conversations!
 Register here
ec.europa.eu/eusurvey/runne...



6 retweets 13 likes

[View all Tweet activity](#)

[View Tweet activity](#)

JAN 2021 SUMMARY

Tweets	Tweet impressions
4	6,979
Profile visits	Mentions
383	6
New followers	
26	

Feb 2021 • 28 days

TWEET HIGHLIGHTS

Top Tweet earned 1,905 impressions
 @sparta_eu and @concordiah2020 joined forces to build an #ecosystem of institutions that provide unique technical resources to partners and cooperate on the organization of #trainings 🤖🤖🤖

Learn more lnkd.in/e3FTyNE
 #cybersecurity #KYPO #CCN
pic.twitter.com/5LgAoOogty



1 retweet 12 likes 13 likes

[View all Tweet activity](#)

[View Tweet activity](#)

Top mention earned 58 engagements



Dr Michael Cooke 🇬🇧🇫🇷🇮🇹🇪🇺
 @MichaelCooke76 · Feb 22
 Funded #ISF @sciencelrel PhD opportunity on Psychology of #CyberSecurity with @deirdre_desmond and me. @AdvanceCrt @ECHOcybersec @Cybersec_EU @BPSCyberPsych @sparta_eu @CyberSecOb @MaynoothUni advance-crt.ie/apply/

1 retweet 1 like 7 likes

[View Tweet](#)

Top media Tweet earned 1,749 impressions

DataBreach: The Good, the bad and the Ugly 🤖 What can we learn from #cyber #criminals? #Leaks have become a significant market and business opportunity 🌐

Learn more sparta.eu/news/2021-01-1...
pic.twitter.com/8Rd9DsaldB



7 retweets 13 likes

[View all Tweet activity](#)

[View Tweet activity](#)


FEB 2021 SUMMARY

Tweets	Tweet impressions
11	15.2K
Profile visits	Mentions
484	17
New followers	
14	

Mar 2021 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 6,248 impressions
 🤖 Why does the industry fail to attract and retain #women in #CyberSecurity ?
 @sparta_eu launched a guide to help companies understand the reasons why and to promote a more #inclusive, #diverse and #attractive workplace.
 sparta.eu/news/2021-03-0...
 pic.twitter.com/fThiMenalc




👤 2 🔄 56 ❤️ 960

[View all Tweet activity](#)

[View Tweet activity](#)

Top mention earned 1,194 engagements
 🤖 Why does the industry fail to attract and retain #women in #CyberSecurity ?
 @sparta_eu launched a guide to help companies understand the reasons why and to promote a more #inclusive, #diverse and #attractive workplace.
 sparta.eu/news/2021-03-0...
 pic.twitter.com/fThiMenalc



👤 2 🔄 56 ❤️ 960


[View all Tweet activity](#)

[View Tweet activity](#)

MAR 2021 SUMMARY


Tweets	8	Tweet impressions	132K
Profile visits	2,604	Mentions	30
New followers	18		

Top Follower followed by 6,187 people



NASK
@NASK_pl
FOLLOWS YOU
[View profile](#)

Top media Tweet earned 3,788 impressions
 Ready to play? The @sparta_eu SAFAIR AI contest is launched! It aims to evaluate the robustness of a #defence technique by means of a two-player game. You can either play in the Attack or Defence tracks.
 Learn more sparta.eu/news/2021-03-0...
 #DeepLearning
 @TU_Muenchen
 pic.twitter.com/OYGBqimXit



👤 7 ❤️ 7


[View all Tweet activity](#)

[View Tweet activity](#)

Apr 2021 • 30 days

TWEET HIGHLIGHTS

Top Tweet earned 2,866 impressions
 The SPARTA Brokerage event is now taking place 🤖
 #partnership #cybersecurity
 pic.twitter.com/dN2DFiSebY



👤 7 ❤️ 11

[View all Tweet activity](#)

[View Tweet activity](#)

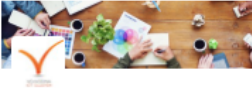
Top mention earned 101 engagements
 🇪🇺 CyberSec_EU
 @Cybersec_EU · Apr 16
 Building up the 🇪🇺 #EU #Cybersecurity Competence Centre: today we hosted the first Informal Governing Board.
 Learn more europa.eu/igC77nK
 @DigitalEU @REA_research @enisa_eu @concordiah2020 @sparta_eu @ecso_eu @ECHOcybersec @cinea_eu @CyberSecEurope @cyberwatchingeu
 twitter.com/LorenaBoix/sta...
 🔄 21 ❤️ 30

[View Tweet](#)

APR 2021 SUMMARY


Tweets	17	Tweet impressions	19.3K
Profile visits	1,357	Mentions	22
New followers	31		

Top Follower followed by 2,660 people



VojvodinaICT cluster
@VOICT
FOLLOWS YOU
Single point of contact with the best #ICT companies in #Serbia.
[View profile](#)

Top media Tweet earned 1,577 impressions
 @sparta_eu Training and Awareness team launched the Curricula Designer, a simple free web-based application that helps education and training providers to design #cybersecurity curricula that reflect needs of current job market 🇪🇺 🤖 🛠️
 Learn more sparta.eu/news/2021-04-0...
 pic.twitter.com/GlifWnXpaD



👤 9 ❤️ 8

[View all Tweet activity](#)

[View Tweet activity](#)

View Tweet activity

May 2021 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 937 impressions
 Don't miss the [#webinar](#) on [#cybersecurity](#) and [#dataprotection!](#) @sparta_eu will be represented by @AnaAyerbe, from our partner @tecnalia

Thank you!! [twitter.com/tecnalia/statu...](https://twitter.com/tecnalia/status/1441111111)

🔗 5 ❤️ 5

[View all Tweet activity](#)

View Tweet activity

Top mention earned 52 engagements
Antonino Sabetta @antoninosabetta · May 24
 Honored to give a lecture at @UniSalerno on secure consumption of #oss at @SAP together with @HenrikPlate and Serena Ponta. Thanks to @fabioalomba3 for the opportunity! @sapopensource #EclipseSteady @AssureMOSSH2020 @sparta_eu #sapsecurityresearch @SAPLabsinFrance


🔗 4 ❤️ 26

[View Tweet](#)

MAY 2021 SUMMARY

Tweets	Tweet impressions
2	6,628
Profile visits	Mentions
740	11
New followers	
16	

Top Follower followed by 2,660 people




VoivodinaICT cluster @VOICT **FOLLOWS YOU**
 Single point of contact with the best #ICT companies in #Serbia.

[View profile](#)

Top media Tweet earned 790 impressions
 📄 A First Look at Android Applications in #GooglePlay related to #COVID19 by @uni_lu & @SnT_uni_lu
 APKcovid evaluates the #security and #efficiency of tracing apps and ensures they do not intrude user #privacy on 📱

Paper available at arxiv.org/abs/2006.11002
pic.twitter.com/KQnK178sfX



🔗 4 ❤️ 7

[View all Tweet activity](#)

View Tweet activity


View Tweet activity

Jun 2021 • 30 days

TWEET HIGHLIGHTS

Top Tweet earned 2,678 impressions
 📄 Discover @sparta_eu's Data Sharing Infrastructure on the integration of 2 main existing sharing platforms: "MISP Threat Sharing" and "C3ISP Collaborative and Confidential Information Sharing and Analysis for Cyber Protection"! sparta.eu/news/2021-06-2...

[#datasharing @CCN_EU](#)
pic.twitter.com/syBHGCMrWj




🔗 7 ❤️ 13

[View all Tweet activity](#)

View Tweet activity

Top mention earned 91 engagements
 📄 Discover @sparta_eu's Data Sharing Infrastructure on the integration of 2 main existing sharing platforms: "MISP Threat Sharing" and "C3ISP Collaborative and Confidential Information Sharing and Analysis for Cyber Protection"! sparta.eu/news/2021-06-2...

[#datasharing @CCN_EU](#)
pic.twitter.com/syBHGCMrWj



🔗 7 ❤️ 13


[View all Tweet activity](#)

View Tweet activity

MAY 2021 SUMMARY

Tweets	Tweet impressions
13	11.2K
Profile visits	Mentions
1,788	23
New followers	
22	

Top Follower followed by 5,321 people




Roberto Di Cosmo @rdicosmo **FOLLOWS YOU**
 Scientist, professor, hacker, writer, citizen. Committed to building a better world through science, technology and community. Director of @swheritage

[View profile](#)

Top media Tweet earned 681 impressions
 📄 SAVE THE DATE! 22 June, one more exciting edition of @secin_lu and @C3_Luxembourg breakfast! This time covering @sparta_eu achievements!

Learn more at breakfast.cybersecurity-luxembourg.com/csb47
pic.twitter.com/U0Teak5mPN



🔗 5 ❤️ 4

[View all Tweet activity](#)

View Tweet activity

Jul 2021 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 1,697 impressions
Morning Readings 📖👍

Through the concept "responsible research and innovation" (by [@EU_Commission](#)[@sparta.eu](#) proposed a process to enable stakeholders to systematically about the possible impacts of the technology they are developing in different dimensions. Learn more [👉 pic.twitter.com/QfphHd9wbn](#)



🔁 9 ❤️ 15

[View all Tweet activity](#)

[View Tweet activity](#)

Top Follower followed by 1,389 people



sundaystar.nft
[@_WEB_SECURITY](#) FOLLOWS YOU
Impressum <https://t.co/d3twmiiA5F>
Datenschutz <https://t.co/MhUuPc8gip...>

[View profile](#)

Top mention earned 146 engagements

Borce Stojkovski
[@b0rce](#) · Jul 28

Inspiring keynotes and interesting talks at the first [@IEEE_CSR](#). Pleasure to present our ongoing work on [@MISPPProject](#) at ACTI, the workshop on Actionable Cyber Threat Intelligence (ACTI) supported by [@ECHOcybersec](#) [@sparta.eu](#) [@concordiah2020](#) [@CyberSec4Europe](#) [pic.twitter.com/7s2H1o1nt9](#)



🔁 2 🗨️ 12 ❤️ 24

[View Tweet](#)

Top media Tweet earned 989 impressions

Save your spot on [@IFIP_PrivacyIdM](#) Summer School, and join junior & senior researchers & practitioners from multiple disciplines to discuss under the [#Privacy](#) and [#Identity #Management!](#) [@sparta.eu](#) & [@CyberSec4Europe](#) hope to see you there! Learn more [👉 sparta.eu/news/2021-07-1...](#) [pic.twitter.com/TUkksDx8L3](#)



🔁 9 ❤️ 7

[View all Tweet activity](#)

[View Tweet activity](#)

JUL 2021 SUMMARY

Tweets	Tweet impressions
6	9,258
Profile visits	Mentions
691	12
New followers	
10	

Aug 2021 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 303 impressions

[@sparta.eu](#) will look closer at the regulation of the situations where personal data security breach has not yet formally occurred, but potentially large-scale vulnerabilities are already known.

Learn more [👉 sparta.eu/news/2021-07-2...](#) [pic.twitter.com/eoMWspVFUP](#)



🔁 4 ❤️ 6

[View all Tweet activity](#)

[View Tweet activity](#)

Top Follower followed by 1,096 people



Giovanni Desiderio
[@Gioooxi](#) FOLLOWS YOU
I'm a millennial, Science-lover and software developer. (Dreamer... with head pain)

[View profile](#)

Top mention earned 18 engagements

IFIP Summer School
[@IFIP_PrivacyIdM](#) · Aug 20

A big thank you to all who made this [#SummerSchool](#) possible!

[@uni_lu](#) [@CyberSec4Europe](#) [@sparta.eu](#) [#EnCaVIBS](#) [@ForumPrivatheit](#) [@ifipnews](#) [#IFIP60](#)

Thanks also to all organizers, PC members, speakers, and participants! [twitter.com/IFIP_PrivacyId...](#)

🔁 1 🗨️ 3 ❤️ 6

[View Tweet](#)

Top media Tweet earned 272 impressions

Save your spot on [@IFIP_PrivacyIdM](#) Summer School, and join junior & senior researchers & practitioners from multiple disciplines to discuss under the [#Privacy](#) and [#Identity #Management!](#) [@sparta.eu](#) & [@CyberSec4Europe](#) hope to see you there! Learn more [👉 sparta.eu/news/2021-07-1...](#) [pic.twitter.com/TUkksDx8L3](#)



🔁 9 ❤️ 7

[View all Tweet activity](#)

[View Tweet activity](#)


AUG 2021 SUMMARY

Tweet impressions	Profile visits
3,006	169
Mentions	New followers
7	8

Sep 2021 - 30 days

TWEET HIGHLIGHTS

Top Tweet earned 2,130 impressions
 We are at @FIC_eu, along with the @concordiah2020, @ECHOcybersec and @CyberSec4Europe!
 Keep posted and keep safe 📺👉
 #h2020 @CCN_EU @Cybersec_ECCC
 pic.twitter.com/EUQmsQ4ack




👤 1 🗨️ 12 ❤️ 30

[View all Tweet activity](#)

[View Tweet activity](#)


Top mention earned 250 engagements
 CyberSec_EU @Cybersec_EU · Sep 7
 Ready for @FIC_eu? Find us at the #EU pavilion of the International Cybersecurity Forum at Lille, France, together with @concordiah2020 @sparta_eu @ECHOcybersec and @CyberSec4Europe
 pic.twitter.com/1x6Wsf1nAY



👤 13 ❤️ 28

[View Tweet](#)

Top media Tweet earned 1,084 impressions
 Another amazing day at @FIC_eu, with @concordiah2020 @ECHOcybersec and @CyberSec4Europe! Together to prepare the @CCN_EU 📺👉
 @Cybersec_EU @Cybersec_ECCC @EU_Commission
 pic.twitter.com/Da2U1Vkeqz



👤 6 ❤️ 25

[View all Tweet activity](#)

[View Tweet activity](#)


SEP 2021 SUMMARY

Tweets	9	Tweet impressions	18.4K
Profile visits	896	Mentions	19
New followers	21		

Oct 2021 - 31 days

TWEET HIGHLIGHTS

Top Tweet earned 471 impressions
 Celebrating #CybersecurityAwarenessMonth with "SPARTA: The Future Needs You!" - an event promoted by @INOvinesc and @VUTvBrne at 📺 to raise awareness on the importance of #cybersecurity and #genderequity! See the event highlights at 📺 instagram.com/s/aGinaGxpZ2h0...
 pic.twitter.com/cVZeKf5avl




👤 6 ❤️ 8

[View all Tweet activity](#)

[View Tweet activity](#)

Top mention earned 34 engagements
 SAVE THE DATE 📺 20 Oct 📺 "Cybersecurity in Higher Education", organised by @NASK_pl & @PolishPlatform and dedicated to @sparta_eu, discusses teaching #cybersecurity at #universities in Poland and abroad.
 Register for free at register.secure.edu.pl
 pic.twitter.com/mN3slZCF1x




👤 1 🗨️ 6 ❤️ 10

[View all Tweet activity](#)

[View Tweet activity](#)

Top media Tweet earned 344 impressions
 "Mathematical science shows what is. It is the language of unseen relations between things. But to use and apply that language, we must be able to fully appreciate, to feel, to seize the unseen, the unconscious."
 📺 Celebrating women in STEM #AdaLovelaceDay
 pic.twitter.com/LV4J4SAnuW



👤 4 ❤️ 8

[View all Tweet activity](#)

[View Tweet activity](#)

OCT 2021 SUMMARY

Tweets	10	Tweet impressions	32.8K
Profile visits	1,391	Mentions	7
New followers	12		

Top Follower followed by 9,611 people
 Télécom SudParis @TelecomSudParis
 Grands école d' #Ingénieurs en #sciences et #technologies de l' #information #IMTFrance. #ingénierie #numérique #recherche #innovation
[View profile](#)

Nov 2021 • 30 days

TWEET HIGHLIGHTS

Top Tweet earned 350 impressions
 GO CYBER WITH SPARTA at **#Madeira**, **#Portugal!** Raising **#CyberSecurityAwareness** across the globe 🌐 Today with **@Escravana** on **#threats** landscape, **#human** aspects on cybersecurity and **#riskmanagement**
 Promoted by **@INOvinesc @UMAGIRP & @EU_Commission**
@Cybersec_ECCC @DigitalEU @enisa
pic.twitter.com/l0rKILJc



🔄 3 ❤️ 10

[View all Tweet activity](#)

[View Tweet activity](#)

Top Follower followed by 2,808 people



Inria Rennes - Bretagne Atlantique
 @Inria_Rennes **FOLLOWS YOU**
 Les sciences du numérique au cœur d'un riche écosystème de **#recherche** et d'**#innovation** ! **#BZH #Bretagne #Inria**

[View profile](#)

Top mention earned 4 engagements

Jason R.C. Nurse
 @jasonnurse · Nov 25
@GroovyHeavy @enisa_eu @Cybersec_EU @CyberSecMonth @Cybersec_ECCC @concordiah2020 @sparta_eu @CyberSec4Europe @DigitalSkillsEU @EUDigitalEdu Very good news indeed! I'm really happy to have contributed as an author to this ENISA research. :-)

🔄 1 ❤️ 1

[View Tweet](#)

Top media Tweet earned 299 impressions

"I didn't see what they saw and they didn't see what I saw. (...) We think a little differently. We perceive things differently."
#genderbalance #CyberSecurity #womenincybersecurity #womenintech

Full article at: sparta.eu/news/2021-11-1-...
pic.twitter.com/mW2FAqSO3B



🔄 5 ❤️ 5

[View all Tweet activity](#)

[View Tweet activity](#)

NOV 2021 SUMMARY

Tweets	3	Tweet impressions	3,436
Profile visits	754	Mentions	5
New followers	22		

Dec 2021 • 31 days

TWEET HIGHLIGHTS

Top Tweet earned 376 impressions
 🚫 DON'T MISS 🚫 This year the **@necsschool** is supported by **@concordiah2020 @CyberSec4Europe @ECHOcybersec** and **@sparta_eu**, with emphasis on the crucial role of **#education** for **#cybersecurity**, proposing new **#training** programmes and **#methods** of teaching 📚
necs-winterschool.disi.unitn.it
pic.twitter.com/H0tO122wIA



🔄 6 ❤️ 4

[View Tweet activity](#)

[View all Tweet activity](#)

Top Follower followed by 2,181 people



Patryk Pawlak
 @patrykpawlak **FOLLOWS YOU**
 Head of Brussels Office **@EU_ISS** | Project Director **@EUCyberDirect** | Editor <https://t.co/ZjeXhUgrE0> | **#EUCyber #DigitalEU** | Usual caveats

[View profile](#)

Top mention earned 23 engagements

TalTech CyberCentre
 @CyberTalTech · Dec 22
 An interesting **#study** report focusing on understanding how **#cybersecurity** recruitment and overall HR processes and motivations work in Europe published as part of the work in **#ECHO #project**.
 Collaboration between **@ecso_eu @concordiah2020 @CyberSec4Europe @ECHOcybersec @sparta_eu** twitter.com/ECHOcybersec/s...

🔄 6 ❤️ 11

[View Tweet](#)

Top media Tweet earned 201 impressions

The SPARTA project wish you a merry Christmas and happy holidays! 🎄🎁 Stay safe in the **#cyberspace!**
pic.twitter.com/L4b6zmPv6J



🔄 2 ❤️ 6

[View Tweet activity](#)

[View all Tweet activity](#)

DEC 2021 SUMMARY

Tweets	5	Tweet impressions	2,580
Profile visits	651	Mentions	2
New followers	6		

Jan 2022 · 31 days

TWEET HIGHLIGHTS

Top Tweet earned 1,465 impressions
 SPARTA #Cybersecurity #hackathon is happening already next week! Meet the amazing mentors that are going to help participants go from an idea to a prototype in 48 hours! lnkd.in/d/TFf6ry
pic.twitter.com/0UXENTOeZd



17 19

[View all Tweet activity](#)

View Tweet activity

Top Follower followed by 3,030 people



Eric Romang
 @eromang FOLLOWS YOU
 @govcert_lu #hcpn #iso27001 #iso27032 #iso22301 #cdpo

[View profile](#)

Top mention earned 42 engagements

MISP
 @MISPProject · Jan 10

A business development hackathon for open source software organised by @secin_lu / @sparta_eu will take place 28-30 January 2022. MISP is included as a potential tool to create new business ideas or startups.

#spartacybersec

eventornado.com/event/spartacy...

8 7

[View Tweet](#)

Top media Tweet earned 655 impressions

PREPARE YOURSELF FOR 48 HOURS FULL OF #HACKING, #CODING, DESIGNING, WORKING WITH TOP-NOTCH EXPERTS, AND THINKING BIG TO SOLVE #CYBERSECURITY CHALLENGES!

SPARTA Cybersecurity Hackathon 28-30 January 2022

Organised by our partner @secin_lu securitymadein.lu/cyber/events/s...
pic.twitter.com/EHN3HFSjNO



6 8

JAN 2022 SUMMARY

Tweets	7	Tweet impressions	4,906
Profile visits	836	Mentions	12
New followers	19		

Feb 2022 · 28 days

TWEET HIGHLIGHTS

Top Tweet earned 1,179 impressions
 Join us for a full day of inspiring and challenging discussions about the #sustainable transition to @Cybersec_ECCEC with the @ECHOcybersec @concordiah2020 @CyberSec4Europe and @EU_Commission, the EU's digital #sovereignty and steps for strengthening #cybersecurity competencies!
pic.twitter.com/hzjBBJC23



1 10 19

[View all Tweet activity](#)

View Tweet activity

Top Follower followed by 11.4K people



Mª Carolina Sanchiz
 @CarolinaSanchiz FOLLOWS YOU
 CryptoArtWoman from 2019. Bichon Maltese Mum. Author. Vegetarian. B2B Marketing Technologist Executive. #DigitalHumanitiesPhD #MIT #ForresterProCX #NFTs

[View profile](#)

Top mention earned 19 engagements

Télécom SudParis
 @TelecomSudParis · Feb 4

*@sparta_eu est un #projet de la Commission européenne, qui a pour but de #développer une action stratégique dans le domaine de la #cybersecurite" indique @herve_debar, dir. de la Recherche et des formations doctorales, membre de @ANSSI_FR. @IMTFrance @IP_Paris. @carnot_tsn

5 6

[View Tweet](#)

Top media Tweet earned 113 impressions

Aug 23 - 26 DONT' MISS SPARTA 2nd International Workshop on Security and Privacy in Intelligent Infrastructures, held in the @ARES_Conference 2022! Speakers from @VUTvBrno @unitartu @BrandonUni Find out the topics and submissions dates at ares-conference.eu/sp2i-2022/



SP2I 2022
 The 2nd International Workshop on Security and Privacy in Intelligent Infrastructures
 An international workshop on the 2nd International Conference on Security and Privacy in Intelligent Infrastructures (SP2I 2022) www.ares-conference.eu

2 5

[View all Tweet activity](#)

View Tweet activity

FEB 2022 SUMMARY

Tweets	6	Tweet impressions	3,221
Profile visits	1,013	Mentions	8
New followers	21		

Mar 2022 · 31 days

TWEET HIGHLIGHTS

Top Tweet earned 1,561 impressions

On the 10 March sit with [@Cybersec_ECCC](#), [@ECHOcybersec](#) [@concordiah2020](#) [@sparta_eu](#), [@CyberSec4Europe](#), [@ecso_eu](#) and [@EU_Commission](#) to discuss #European #cybersecurity #sustainability

Learn more at [Inkd.in/dkDTs8qP](#)
And register here [Inkd.in/dtFajGpD](#)
[pic.twitter.com/fovSag6gN](#)



5 12 13

[View all Tweet activity](#)

[View Tweet activity](#)

Top mention earned 92 engagements

On the 10 March sit with [@Cybersec_ECCC](#), [@ECHOcybersec](#) [@concordiah2020](#) [@sparta_eu](#), [@CyberSec4Europe](#), [@ecso_eu](#) and [@EU_Commission](#) to discuss #European #cybersecurity #sustainability

Learn more at [Inkd.in/dkDTs8qP](#)
And register here [Inkd.in/dtFajGpD](#)
[pic.twitter.com/fovSag6gN](#)



5 12 13

[View all Tweet activity](#)

[View Tweet activity](#)

MAR 2022 SUMMARY

Tweets	Tweet impressions
7	5,870
Profile visits	Mentions
1,486	18
New followers	
8	

Top media Tweet earned 304 impressions

August 23 to 26 Prepare yourself for [@sparta_eu](#) Workshop on Education, Training and Awareness in Cybersecurity to be held in conjunction with the 17th ARES Conference. The workshop will be chaired the amazing [@JanHajny3](#) from [@VUTvBrno](#)

Learn more [ares-conference.eu/workshops-eu-s...](#)
[pic.twitter.com/0lzcYUtvjx](#)



ETACS 2022
Workshop on Education, Training and Awareness in Cybersecurity ETACS 2022
Institutional contact information: "ETACS" - European Conference on Cyber Security and Security
2022 (2021) [http://www.ares-conference.eu](#)
April 01, August 01, 2022

5 11

[View all Tweet activity](#)

[View Tweet activity](#)

APR 2022 SUMMARY

Tweets	Tweet impressions
3	2,705
Profile visits	Mentions
1,010	28
New followers	
13	

Apr 2022 · 30 days

TWEET HIGHLIGHTS

Top Tweet earned 1,177 impressions

[@yeswehack](#) [@doctolib](#) [@BlaBlaCar](#) [@Malt_France](#) & [@sparta_eu](#) launch the first live Bug Bounty event dedicated to #European scale-ups and #unicorns! Hack Me I'm Famous - 13 & 14 April - hosts a SPARTA workshop with #ethicalcommunity to discuss contributions to the [#cybersecurity](#) [pic.twitter.com/vYqzzgZ1rT](#)



4 12

[View all Tweet activity](#)

[View Tweet activity](#)

Top mention earned 454 engagements

[YesWeHack](#) [@yeswehack](#) · Apr 13
 Here we go! Our 30-hour live #BugBounty Hack Me I'm Famous at [@CampusCyberFr](#) has just begun. Thanks again to our partners [@doctolib](#), [@BlaBlaCar_FR](#), [@Malt_France](#), [@sparta_eu](#) and to the hunters who joined us!

Learn more here [hackmeimfamous.com/#hack-me](#)

#HMIF #YesWeRHackers
[pic.twitter.com/ELbuhPYc4B](#)



1 7 42

[View Tweet](#)

Top media Tweet earned 240 impressions

SAVE THE DATE for the next CONVERGENCE event 1-3 June, Brussels [cybercompetencenetwork.eu/convergence-ne...](#)

[@CyberSec4Europe](#) [@concordiah2020](#) [@ECHOcybersec](#) [@sparta_eu](#) [@EU_Commission](#)
[pic.twitter.com/OrnQ25lyl8](#)



5 6

Top Follower followed by 1,472 people



Nicolas Verdier
[@n1nj4sec](#) · FOLLOWS YOU
Hacker | Bug Bounty Hunter | Cyber Security Consultant

[View profile](#)

May 2022 • 29 days so far...

TWEET HIGHLIGHTS

Top Tweet earned 497 impressions

SAVE THE DATE 📅 20-22 May
 @Technoport_Lux
 #BusinessDevelopment #Hackathon for building products from available #cybersecurity #opensource tools! Up to 12 teams will compete and use #tools developed under @sparta_eu and @concordiah2020
 Inkd.in/eJUaHpTY
 twitter.com/secin_lu/statu...
 pic.twitter.com/ffc9lhnd6N



🔗 8 ❤️ 7

[View all Tweet activity](#)

View Tweet activity

Top Follower followed by 96.4K people



Brenda Hill Skystad
 @realBSkystad FOLLOWS YOU
 WA state's 1989 Whistleblower law is named after me. 1st in the USA. Please google Brenda Hill whistleblower stories. 33 states so far. followed by @kevincorke

[View profile](#)

Top mention earned 46 engagements

securitymadein.lu
 @secin_lu · Apr 28
 #BusinessDevelopment #Hackathon for building products from available #cybersecurity #opensource tools.
 📅 20-22 May 2022
 @Technoport_Lux

👥 Up to 12 teams will compete and use tools developed under @sparta_eu and @concordiah2020

REGISTER NOW! en.xing-events.com/PSJQTK.html

🔗 1 🔁 10 ❤️ 7

[View Tweet](#)

Top media Tweet earned 233 impressions

CONVERGENCE NEXT is all about @Cybersec_ECCC and the future of #cybersecurity! High-level representatives from 🇪🇺 institutions will discuss the role of the ECCC and the next stages for the wider stakeholder community. Register now!!! 🇪🇺 eu.hessen.de/event.php?vnr=... pic.twitter.com/5HYkqdlAbS



🔗 2 ❤️ 2

[View all Tweet activity](#)

MAY 2022 SUMMARY

Tweets	Tweet impressions
6	1,741
Profile visits	Mentions
949	10
New followers	
13	

Bibliography

[1]

Hutchinson, A. (2020, 01 08). *Twitter Is Removing the Audience Insights Element from Twitter Analytics*. Retrieved from Social Media Today: <https://www.socialmediatoday.com/news/twitter-is-removing-the-audience-insights-element-from-twitter-analytics/569982/>