Cyber Security for Europe

D9.10

Report on the Outreach and Dissemination Activities 2

Document Identification	
Due date	31st January 2021
Submission date	29st January 2021
Revision	1.1 (20 May 2021)

Related WP	WP9	Dissemination Level	PU
Lead Participant	UMA	Lead Author	Carmen Fernandez-Gago (UMA)
Contributing Beneficiaries	TDL, UMA	Related Deliverables	D9.3, 9.5, D9.23

Abstract: This document describes the outreach activities, that is, the dissemination and communication activities carried out by the CyberSec4Europe partners during the second year of the project. These activities are in alignment with the project's Dissemination and Awareness Plan.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This report is the second in a series of deliverables based on the work done in WP9, more specifically in T9.2, covering the outreach activities of all the partners and provides details of the dissemination and communication activities of the CyberSec4Europe project during the second year. These activities follow the strategy for communication and dissemination of the project, published in August 2019. Even though the strategy was designed before the COVID-19 pandemic, it was not considered necessary to update it as many of the activities could be carried out online. Thus, as the strategy plan identifies different target audiences and different dissemination and communication channels, this document aligns with that classification.

Document information

Contributors

Name	Partner
Carmen Fernandez-Gago	UMA
Javier Lopez	UMA
David Goodman	TDL

Reviewers

Name	Partner
Stephan Krenn	AIT
Pasquale Annicchino	ARCH

History

0.01	2020-11-03	Carmen Fernandez-Gago	Proposed table of contents
v0.1	2020-12-02	Carmen Fernandez-Gago	First draft
v0.2	2021-01-19	Carmen Fernandez-Gago, Javier Lopez	First version sent for review
v0.3		Carmen Fernandez-Gago	Reviewer comments addressed
v1.0	2021-01-25	David Goodman, Carmen Fernandez-Gago	Completed content for Section 4. Final version ready for submission
v1.1	2021-05-10	David Goodman, Carmen Fernandez-Gago	Addition of section on hackathons and pitstops
v1.1	2021-05-20	Ahad Niknia	Final check, preparation and submission process

List of Contents

1 Introduction 1
2 Dissemination and Outreach Activities 2
2.1 Social 2
2.2 Technical 2
2.3 Scientific 2
2.3.1 Articles in Journals 2
2.3.2 Articles at Conferences 4
2.3.3 Book Chapters 7
2.3.4 Summer Schools 7
2.3.5 Organisation of Events (Conference and Workshops) 8
2.3.6 Presentations at Events 8
2.3.7 Hackathons and Pitstops 10
2.4 Business 10
2.5 Governmental 11
2.6 Standardisation 12
3 Achievement of KPI Indicators 15
4 Joint Activities with the other Three Pilots 17
5 Conclusion 18
6 References 19

List of Tables

Table 1 Key Performance Indicator results up to M24 16

List of Acronyms

AIT	Austrian Institute of Technology GmbH
BRNO	Masaryk University
CCN	Cybersecurity Competence Centre
CNR	National Research Council (Consiglio Nazionale delle Ricerche)
CONCORDIA	Cybersecurity Competence for Research and Innovation
CYBER	Cybernetica
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DIN	German Institute of Standardisation (translation to English from German)
DTU	Technical University of Denmark
ECHO	European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations
ECSO	European Cyber Security Organisation
EDPS	European Data Protection Supervisor
EU	European Union
GUF	Goethe University Frankfurt
I-BP	Informatique Banques Populaires
INCIBE	Insitituto de Cyberseguridad
JAMK	Jyväskylä University of Applied Sciences
JRC	Joint Research Centre
KAU	Karlstad University
KPI	Key Performance Indicator
NIA	Information Technology and Applications
OASC	Open & Agile Smart Cities
REA	Research Executive Agency
SIE	Siemens
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
TDL	Trust in Digital Life
TLEX	Timelex
TUD	Technical University of Delft
UCD	University College Dublin
UCY	University of Cyprus
UM	University of Maribor
UMA	University of Malaga
UMU	University of Murcia
UNITN	University of Trento
UPRC	University of Piraeus Research Centre
UPS-IRIT	Université Paul Sabatier Toulouse III
VTT	Teknologian tutkimuskeskus VTT Oy

WG	Working Group

1 Introduction

CyberSec4Europe is, together with CONCORDIA, ECHO and SPARTA, working to create a coordinated network of experts in the field of cybersecurity who are able to determine the best practices needed in order to respond to failures or attacks that would hamper the development of a Digital Single Market. The work of these projects will be the seed for the creation of a cybersecurity competence network with a European Cybersecurity Research and Competence Centre.

Given the importance of the key objectives of CyberSec4Europe, it is crucial how its partners communicate the project's research and innovation. It must explain to the citizens of Europe how the outcomes of its work are relevant to their everyday lives, through improving their security and economic well-being. The project must spread its results so that policy makers are better informed and that the rest of the scientific community and industry can benefit from this work.

According to [D9.3] the benefits of effective dissemination and awareness are the ability to:

- draw the attention of national and regional governments, and potentially other public and private funding sources, to the work of the pilot;
- attract the interest of potential partners;
- attract first rate students and scientists to join the partners' institutes and enterprises;
- enhance the standing and visibility of the partners, both at a national and international level;
- assist with the search for financial backers to exploit results.

Thus, in order to achieve the effective communication mentioned above in a successful manner, the project's dissemination and awareness strategy identified an appropriate set of target audiences which are: social, technical, scientific, business, legislative and standardisation bodies.

([D9.3]) also identified the main communication and dissemination channels that are to be used to reach these target audiences.

In this deliverable we have followed the classification in audience categories given above for listing details of all the communication activities that have been carried out, specifying the main channel used for each. We have compared the achievements on dissemination and communication with the key performance indicators established in the strategy document as indicators of success and have stated that, for most of the KPIs. Even though the situation of the pandemic the dissemination activities have accommodated in most of the cases to online events. This has allowed that CyberSec4Europe has not stopped spreading the word as the technical work has not stopped neither.

Thus, the structure of this deliverable is as follows. Section 2 describes these activities according to the target audiences identified. In Section 3 we compare the achievements of CyberSec4Europe against the KPIs in [D9.3]. Section 4 describes the activities that have been carried out done in collaboration with the other three pilots and Section 5 provides our conclusions.

2 Dissemination and Outreach Activities

In this section we describe how the target audiences that we identified in D9.5 were approached by the project partners. Even though COVID-19 has had a continuing impact on face-to-face dissemination events, we all adapted to the new situation and many events were carried out online. We specify for each of these events the communication channel that was used.

2.1 Social

Many of the results and activities of CyberSec4Europe are communicated through the website [D9.9], press releases, events and exhibitions. These activities include:

1. ATOS included the CyberSec4Europe project in the annual version of Atos Research & Innovation Booklet 2019 published in April 2020.
2. ATOS participation in event/webinar organised by INCIBE titled: New challenges, new opportunities in cybersecurity (Telecommunications, Training, Industry, and Transportation, Madrid, June 2020.
3. BRNO delivered a lecture discussing the importance of vulnerabilities search in cryptographic devices and need for more transparency in security certification, online, November 2020.
4. Public event of CyberSec4Europe meeting including an evening panel discussion, Brussels, February 2020.
5. Public event of CyberSec4Europe with an evening panel discussion, "Realising Europe's Cybersecurity Strengths and Capacity for the 2020s", online, July 2020.
6. UMA took part in the event organized for civil society in Malaga on 'ICT, Crime and COVID-19', online, May 2020.
7. UPRC was a keynote speaker presenting the challenges and risks of the Internet of Things in the Internet Safety event held in Cyprus, February 2020. They participated as well in several follow-up discussions emphasizing on the importance of projects like CyberSec4Europe.

2.2 Technical

1. BRNO presented the Cyber Sandbox Creator, a part of virtual lab for open-source tools education and research, at CCN Webinar on Cyber Ranges, online, June 2020.

2.3 Scientific

All the publications are open access through the project website.

2.3.1 Articles in Journals

1. Krenn,Stephan, Henrich C. Pöhls, Kai Samelin, Daniel Slamanig. *Fully invisible protean signatures schemes.* IET Information Security(2020), 14 (3): 266. http://dx.doi.org/10.1049/iet-ifs.2019.0141
2. Daoudagh, S., Lonetti, F. & Marchetti, E. *XACMET: XACML Testing & Modeling*. Software Qual J 28, 249–282 (2020). https://doi.org/10.1007/s11219-019-09470-5

3. Said Daoudagh, Francesca Lonetti and Eda Marchetti. *An automated framework for continuous development and testing of access control systems*. Journal of Software: Evolution And Process. John Wiley & Sons Ltd ("Wiley"), e2306, 2020.
4. Harborth, D.; Pape, S. and Rannenberg, K. *Explaining the Technology Use Behavior of Privacy-Enhancing Technologies: The Case of Tor and JonDonym*. In Proceedings on Privacy Enhancing Technologies (PoPETs), volumen 2020, Issue 2. http://dx.doi.org/10.2478/popets-2020-0020 .
5. Pape, S.; Paci, F.; Juerjens, J. and Massacci, F. *Selecting a Secure Cloud Provider: An Empirical Study and Multi Criteria Approach*, Journal of Information 11(5), MDPI, 2020 http://dx.doi.org/10.3390/info11050261
6. J. E. Rubio, R. Roman and J. Lopez, '*Integration of a Threat Traceability Solution in the Industrial Internet of Things'* in IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6575-6583, Oct. 2020, doi: 10.1109/TII.2020.2976747.
7. A. Nieto, "Becoming JUDAS: *Correlating Users and Devices During a Digital Investigation*, in IEEE Transactions on Information Forensics and Security, vol. 15, pp. 3325-3334, 2020, doi: 10.1109/TIFS.2020.2988602.
8. Davy Preuveneers, Wouter Joosen, Jorge Bernal Bernabe, Antonio Skarmeta, *Distributed Security Framework for Reliable Threat Intelligence Sharing*, Security and Communication Networks, vol. 2020, Article ID 8833765, 15 pages, 2020. https://doi.org/10.1155/2020/8833765
9. Marko Kompara, Tomi Jerenko, Marko Hölbl. *Primerjava hitrosti simetričnih bločnih šifer.* Uporabna Informatika.
10. Cristina Alcaraz, Juan E. Rubio, Javier Lopez, *Blockchain-assisted access for federated Smart Grid domains: Coupling and features*, Journal of Parallel and Distributed Computing, Volume 144, 2020, Pages 124-135, ISSN 0743-7315, https://doi.org/10.1016/j.jpdc.2020.05.012.
11. Ferraris, D., Bastos, D., Fernandez-Gago, C. et al. *A trust model for popular smart home devices*. Int. J. Inf. Secur. (2020). https://doi.org/10.1007/s10207-020-00519-2
12. Ferraris, D., Fernandez-Gago, C. & Lopez, J. *A model-driven approach to ensure trust in the IoT*. Hum. Cent. Comput. Inf. Sci. 10, 50 (2020). https://doi.org/10.1186/s13673-020-00257-3
13. M. Kolar, C. Fernandez-Gago, and J. Lopez, *A Model Specification Implementation for Trust Negotiation*, The 14th International Conference on Network and System Security (NSS 2020), vol. 12570, Springer, pp. 327-341, 11/2020.
14. Matheu, S.N.; Robles Enciso, A.; Molina Zarca, A.; Garcia-Carrillo, D.; Hernández-Ramos, J.L.; Bernal Bernabe, J.; Skarmeta, A.F. *Security Architecture for Defining and Enforcing Security Profiles in DLT/SDN-Based IoT Systems*. Sensors 2020, 20, 1882.
15. Sara N. Matheu, José L. Hernández-Ramos, Antonio F. Skarmeta, Gianmarco Baldini. *A Survey of Cybersecurity Certification for the Internet of Things*. ACM Computer Surveys, vol. 56, no. 3, 2020. DOI: 10.1145/3410160
16. Norberto Garcia, Tomas Alcaniz, Aurora González-Vidal, Jorge Bernal Bernabe, Diego Rivera, Antonio Skarmeta. *Distributed real-time SlowDoS attacks detection over encrypted traffic using Artificial Intelligence*, Journal of Network and Computer Applications, Volume 173, 2021, 102871, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102871.
17. A. Hermosilla, A. M. Zarca, J. B. Bernabe, J. Ortiz and A. Skarmeta, *Security Orchestration and Enforcement in NFV/SDN-Aware UAV Deployments*, in IEEE Access, vol. 8, pp. 131779-131795, 2020, doi: 10.1109/ACCESS.2020.3010209.

18. Zarca AM, Bagaa M, Bernabe JB, Taleb T, Skarmeta AF. *Semantic-Aware Security Orchestration in SDN/NFV-Enabled IoT Systems*. Sensors (Basel). 2020 Jun 27;20(13):3622. doi: 10.3390/s20133622. PMID: 32605111; PMCID: PMC7374451.
19. Molina Zarca, A.; Bagaa, M.; Bernal Bernabe, J.; Taleb, T.; Skarmeta, A.F. *Semantic-Aware Security Orchestration in SDN/NFV-Enabled IoT Systems*. Sensors 2020, 20, 3622.
20. Marko Kompara, Tomi Jerenko, Marko Hölbl. *Primerjava hitrosti simetričnih bločnih šifer*. Uporabna Informatika, 2020.
21. Mark Kuper, Fabio Massacci, Woohyun Shim, Julian Williams. *Who Should Pay for Interdependent Risk? Policy Implications for Security Interdependence Among Airports*. Journal of Risk Analysis, volume 40(5), pp. 1001-1019, May 2020, Wiley.
22. I. Pashchenko, H. Plate, S. E. Ponta, A. Sabetta and F. Massacci, *Vuln4Real: A Methodology for Counting Actually Vulnerable Dependencies*, in IEEE Transactions on Software Engineering, doi: 10.1109/TSE.2020.3025443.
23. F. Massacci and N. Ngo, *Distributed Financial Exchanges: Security Challenges and Design Principles* in IEEE Security & Privacy, vol. , no. 01, pp. 0-0, 5555. doi: 10.1109/MSEC.2020.2994826
24. Constantinos Patsakis, Fran Casino, Vasilios Katos, *Encrypted and covert DNS queries for botnets: Challenges and countermeasures*, Computers & Security, Volume 88, 2020, 101614, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2019.101614.
25. Hurley-Smith, Darren, Patsakis, Constantinos, Hernandez-Castro, Julio C. (2020) *On the unbearable lightness of FIPS 140-2 randomness tests.* IEEE Transactions on Information Forensics and Security, . p. 1. ISSN 1556-6013. 10.1109/TIFS.2020.2988505
26. Papastergiou, S., Mouratidis, H. & Kalogeraki, EM. *Handling of advanced persistent threats and complex incidents in healthcare, transportation and energy ICT infrastructures*. Evolving Systems (2020). https://doi.org/10.1007/s12530-020-09335-4
27. Theodoros Apostolopoulos, Vasilios Katos, Kim-Kwang Raymond Choo, Constantinos Patsakis, *Resurrecting anti-virtualization and anti-debugging: Unhooking your hooks*, Future Generation Computer Systems, Volume 116, 2021, Pages 393-405, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.11.004.
28. C. Patsakis, F. Casino, N. Lykousas and V. Katos, *Unravelling Ariadne's Thread: Exploring the Threats of Decentralised DNS*, in IEEE Access, vol. 8, pp. 118559-118571, 2020, doi: 10.1109/ACCESS.2020.3004727.
29. Eugenia A. Politou, Efthimios Alepis, Constantinos Patsakis, Fran Casino, Mamoun Alazab. *Delegated content erasure in IPFS*, Future Generation Computer Systems, volume 112, pp. 956-964, Elsevier 10.1016/j.future.2020.06.037
30. Pascoal, Túlio; Decouchant, Jérémie; Boutet, Antoine; Esteves-Verissimo, Paulo, *DyPS: Dynamic, Private and Secure GWAS*, Sciendo 2020.
31. Jayavarshini Thirumalai. *An integrated approach for certification and re-certification based on the case study of an integrated circuit*, MSc thesis, University of Tartu, January 2021 https://comserv.cs.ut.ee/ati_thesis/datasheet.php?id=71069&year=2021

2.3.2 Articles at Conferences

1. Jan Bobolz, Fabian Eidens, Stephan Krenn, Daniel Slamanig, Christoph Striecks. *Privacy-Preserving Incentive Systems with Highly Efficient Point-Collection*. ACM ASIA Conference on Computer and

Communications Security ASIA CCS. October 2020 Pages 319–333. https://doi.org/10.1145/3320269.3384769.

2. V. Mavroudis and P. Svenda, *JCMathLib: Wrapper Cryptographic Library for Transparent and Certifiable JavaCard Applets*, 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 2020, pp. 89-96, doi: 10.1109/EuroSPW51379.2020.00022.
3. Janovsky A., Nemec M., Svenda P., Sekan P., Matyas V. (2020) *Biased RSA Private Keys: Origin Attribution of GCD-Factorable Keys*. In: Chen L., Li N., Liang K., Schneider S. (eds) Computer Security – ESORICS 2020. ESORICS 2020. Lecture Notes in Computer Science, vol 12309. Springer, Cham. https://doi.org/10.1007/978-3-030-59013-0_25
4. Sedlacek V., Jancar J., Svenda P. (2020) *Fooling Primality Tests on Smartcards*. In: Chen L., Li N., Liang K., Schneider S. (eds) Computer Security – ESORICS 2020. ESORICS 2020. Lecture Notes in Computer Science, vol 12309. Springer, Cham. https://doi.org/10.1007/978-3-030-59013-0_11
5. Jancar, J., Sedlacek, V., Svenda, P., & Sys, M. (2020). *Minerva: The curse of ECDSA nonces : Systematic analysis of lattice attacks on noisy leakage of bit-length of ECDSA nonces*. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(4), 281-308. https://doi.org/10.13154/tches.v2020.i4.281-308
6. Sousa P.R., Martins R., Antunes L. (2020) *Empowering Users Through a Privacy Middleware Watchdog*. In: Gritzalis S., Weippl E.R., Kotsis G., Tjoa A.M., Khalil I. (eds) Trust, Privacy and Security in Digital Business. TrustBus 2020. Lecture Notes in Computer Science, vol 12395. Springer, Cham. https://doi.org/10.1007/978-3-030-58986-8_11
7. Brandão A., Resende J.S., Martins R. (2020) *Employment of Secure Enclaves in Cheat Detection Hardening*. In: Gritzalis S., Weippl E.R., Kotsis G., Tjoa A.M., Khalil I. (eds) Trust, Privacy and Security in Digital Business. TrustBus 2020. Lecture Notes in Computer Science, vol 12395. Springer, Cham. https://doi.org/10.1007/978-3-030-58986-8_4
8. Patrícia R. Sousa, João S. Resende, Rolando Martins, Luís Antunes. *The case for blockchain in IoT identity management.* Journal of Enterprise Information Management, volumen 33, 2020.
9. Said Daoudagh, Francesca Lonetti and Eda Marchetti. *Assessing Testing Strategies for Access Control Systems: A Controlled Experiment.* Proceedings of the 6th International Conference on Information Systems Security and Privacy, (ICISSP 2020), Volume 1: ICISSP, 107-118, 2020, Valletta (Malta).
10. Said Daoudagh and Eda Machetti. *Defining Controlled Experiments Inside the Access Control Environment.* Proceedings of the 8th International Conference on Model-Driven Engineering and Software Development, (MODELSWARD 2020), 25 February 2020, 167-176, 2020, Valletta (Malta).
11. Said Daoudagh and Eda Machetti. *A Life Cycle for Authorization Systems Development in the GDPR Perspective*. Proceedings of the Fourth Italian Conference on Cyber Security, February 2020, pp. 128-140. http://ceur-ws.org/Vol-2597/paper-12.pdf , Ancona (Italy).
12. Barsocchi P. et al. (2020). *A Privacy-By-Design Architecture for Indoor Localization Systems.* In: Shepperd M., Brito e Abreu F., Rodrigues da Silva A., Pérez-Castillo R. (eds) Quality of Information and Communications Technology. QUATIC 2020. Communications in Computer and Information Science, vol 1266. Springer, Cham. https://doi.org/10.1007/978-3-030-58793-2_29
13. Maurice H. ter Beek, Axel Legay, Alberto Lluch-Lafuente, Andrea Vandin. *Variability meets security: quantitative security modeling and analysis of highly customizable attack scenarios.* VAMOS '20: Proceedings of the 14th International Working Conference on Variability Modelling of Software-Intensive SystemsFebruary 2020 Article No.: 11 Pages 1–9, ACM.

14. Anders Schlichtkrull, Sebastian Mödersheim. *Accountable Trust Decisions: A Semantic Approach.* Open Identity Summit 2020, Gesellschaft für Informatik e.V.
15. John Korniotakis, Panagiotis Papadopoulos, and Evangelos Markatos. *Beyond Black and White: Combining the Benefits of Regular and Incognito Browsing Modes.* Proceedings of the 17th International Joint Conference on e-Business and Telecommunications - Volume 3: SECRYPT, pp. 192-200, Scitepress.
16. Christodoulaki, M., Esposito, S.M., Mantelero, A., Monte, A., Vaciago, G., *Fostering cybersecurity in Europe through regulation*. In Joan Balcells et al. Cybercrime: new threats, new responses. Proceedings of the XVth International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya, Barcelona, 1-2 July, 2020, 104-125
17. Schmitz C., Sekulla A., Pape S. (2020) *Asset-Centric Analysis and Visualisation of Attack Trees*. In: Eades III H., Gadyatskaya O. (eds) Graphical Models for Security. GraMSec 2020. Lecture Notes in Computer Science, vol 12419. Springer, Cham. https://doi.org/10.1007/978-3-030-62230-5_3
18. Hazilov V., Pape S. (2020) *Systematic Scenario Creation for Serious Security-Awareness Games.* In: Boureanu I. et al. (eds) Computer Security. ESORICS 2020. Lecture Notes in Computer Science, vol 12580. Springer, Cham. https://doi.org/10.1007/978-3-030-66504-3_18
19. Pape S., Goeke L., Quintanar A., Beckers K. (2020) *Conceptualization of a CyberSecurity Awareness Quiz*. In: Hatzivasilis G., Ioannidis S. (eds) Model-driven Simulation and Training Environments for Cybersecurity. MSTEC 2020. Lecture Notes in Computer Science, vol 12512. Springer, Cham. https://doi.org/10.1007/978-3-030-62433-0_4
20. von Wintzingerode, C.; Müllmann, D. *Ein europäisches Netzwerk für Cybersicherheit*. Tagungsband Herbstakademie 2020: Den Wandel begleiten. IT-rechtliche Herausforderungen der Digitalisierung, pp. 475-492
21. Fischer-Hübner S. et al. (2020) *Quality Criteria for Cyber Security MOOCs*. In: Drevin L., Von Solms S., Theocharidou M. (eds) Information Security Education. Information Security in Action. WISE 2020. IFIP Advances in Information and Communication Technology, vol 579. Springer, Cham. https://doi.org/10.1007/978-3-030-59291-2_4
22. Garofalo G., Preuveneers D., Joosen W. (2020) *Data Privatizer for Biometric Applications and Online Identity Management.* In: Friedewald M., Önen M., Lievens E., Krenn S., Fricker S. (eds) Privacy and Identity Management. Data for Better Living: AI and Privacy. Privacy and Identity 2019. IFIP Advances in Information and Communication Technology, vol 576. Springer, Cham. https://doi.org/10.1007/978-3-030-42504-3_14
23. Preuveneers D., Joosen W. (2020) *TATIS: Trustworthy APIs for Threat Intelligence Sharing with UMA and CP-ABE*. In: Benzekri A., Barbeau M., Gong G., Laborde R., Garcia-Alfaro J. (eds) Foundations and Practice of Security. FPS 2019. Lecture Notes in Computer Science, vol 12056. Springer, Cham. https://doi.org/10.1007/978-3-030-45371-8_11
24. Rubio J.E., Alcaraz C., Rios R., Roman R., Lopez J. (2020) *Distributed Detection of APTs: Consensus vs. Clustering*. In: Chen L., Li N., Liang K., Schneider S. (eds) Computer Security – ESORICS 2020. ESORICS 2020. Lecture Notes in Computer Science, vol 12308. Springer, Cham. https://doi.org/10.1007/978-3-030-58951-6_9
25. J. L. Hernández-Ramos, G. Baldini, S. N. Matheu and A. Skarmeta, *Updating IoT devices: challenges and potential approaches*, 2020 Global Internet of Things Summit (GIoTS), Dublin, Ireland, 2020, pp. 1-5, doi: 10.1109/GIOTS49054.2020.9119514
26. F. Alrimawi, L. Pasquale, D. Mehta, N. Yoshioka and B. Nuseibeh, *Incidents Are Meant for Learning, Not Repeating: Sharing Knowledge About Security Incidents in Cyber-Physical Systems* in IEEE Transactions on Software Engineering, vol. , no. 01, pp. 1-1, 5555. https://doi.ieeecomputersociety.org/10.1109/TSE.2020.2981310

27. S. Ali Mirheidari, S. Arshad , K. Onarlioglu, B. Crispo, E. Kirda, W. Robertson. *Cached and Confused: Web Cache Deception in the Wild*. USENIX Security Symposium, Boston, MA, USA, August 2020.
28. Duc Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, Antonino Sabetta. *Towards Using Source Code Repositories to Identify Software Supply Chain Attacks*. CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications SecurityOctober 2020 Pages 2093–2095 https://doi.org/10.1145/3372297.3420015
29. G. Di Tizio, F. Massacci, L. Allodi, S. Dashevskyi and J. Mirkovic, *An Experimental Approach for Estimating Cyber Risk: a Proposal Building upon Cyber Ranges and Capture the Flags*, 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 2020, pp. 56-65, doi: 10.1109/EuroSPW51379.2020.00016.
30. G. Di Tizio and C. Nam Ngo, *Are You a Favorite Target For Cryptojacking? A Case-Control Study On The Cryptojacking Ecosystem*, 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 2020, pp. 515-520, doi: 10.1109/EuroSPW51379.2020.00075.
31. Ivan Pashchenko, Duc Ly Vu, Fabio Massacci. *A Qualitative Study of Dependency Management and Its Security Implications. CCS '20:* Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. October 2020 Pages 1513–1531 https://doi.org/10.1145/3372297.3417232
32. Duc Ly Vu, Ivan Pashchenko, Fabio Massacci, Henrik Plate, Antonino Sabetta. *Typosquatting and Combosquatting Attacks on the Python Ecosystem.* 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). 10.1109/EuroSPW51379.2020.00074
33. Ivan Pashchenko, Duc Ly Vu, Fabio Massacci. *Preliminary Findings on FOSS Dependencies and Security A Qualitative Study on Developers' Attitudes and Experience*. ICSE '20: Proceedings of the ACM/IEEE 42nd International Conference on Software Engineering: Companion ProceedingsJune 2020 Pages 284–285 https://doi.org/10.1145/3377812.3390903
34. C. N. Ngo, D. Friolo, F. Massacci, D. Venturi and E. Battaiola, Vision: *What If They All Die? Crypto Requirements For Key People*, 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy, 2020, pp. 178-183, doi: 10.1109/EuroSPW51379.2020.00032.
35. Broders N., Martinie C., Palanque P., Winckler M., Halunen K. (2020) *A Generic Multimodels-Based Approach for the Analysis of Usability and Security of Authentication Mechanisms*. In: Bernhaupt R., Ardito C., Sauer S. (eds) Human-Centered Software Engineering. HCSE 2020. Lecture Notes in Computer Science, vol 12481. Springer, Cham. https://doi.org/10.1007/978-3-030-64266-2_4
36. Rouland Q., Hamid B., Jaskolka J. (2020) *Reusable Formal Models for Threat Specification, Detection, and Treatment.* In: Ben Sassi S., Ducasse S., Mili H. (eds) Reuse in Emerging Software Engineering Practices. ICSR 2020. Lecture Notes in Computer Science, vol 12541. Springer, Cham. https://doi.org/10.1007/978-3-030-64694-3_4

2.3.3 Book Chapters

- Sara Nieves Matheu, Antonio Skarmeta. *Cybersecurity Certificationin IoT Environments.* In Security Risk Management For The Internet Of Things, now Publishers Inc, 2020.

2.3.4 Summer Schools

Here we list the summer schools at which CyberSec4Europe partners participated. Details can be found in [D9.7] and in the forthcoming [D9.16].

- A PhD student in CNR delivered a talk on 'The GDPR Compliance through Authorization Systems' at the TAROT summer school, 16th International Summer School on Training And Research On Testing. The school took place in Porto, October 2020.

- IFIP Summer School on Privacy and Identity Management, online, 20-23 September 2020
  - General Chair: AIT
  - Steering Committee chaired by GUF, BRNO and KAU
  - Several CyberSec4Europe partners were on the Progam Committee co-chaired with SPARTA. .

2.3.5 Organisation of Events (Conference and Workshops)

- JAMK organised *Flagship 1: An Online Cybersecurity Exercise*, online, 12-13 January 2021.
- AIT was the General Chair of the International Conference on Cryptology and Network Security (CANS 2020), online, 30 October 2020.
- C3P and GUF were among the organisers of the ENISA Annual Privacy Forum 2020, online, October 2020.
- DTU organised the Open Identity Summit 2020, online publication event.
- UM and GUF organised the 35th International Conference on Information Security and Privacy Protection IFIP Sec 2020, online, September 2020.
  - The IFIP Summer School on Privacy and Identity Management 2020 (General Chair: AIT) was co-located with IFIP Sec 2020
- TUD organised the workshop Understanding Data-Sharing and Collaboration, online, August 2020.
- UMA has been involved in the following online events:
  - 15th International Conference on Wireless Algorithms, Systems, and Applications, September 12-15 2020.
  - 2nd International Workshop on Information Security Methodology and Replication Studies, 25-28 August 2020.
  - 25th Australasian Conference on Information Security and Privacy, 30 November-2 December 2020 .
  - European Interdisciplinary Cybersecurity Conference, 18 November 2020.
  - 17th International Conference on Security and Cryptography, 8-10 July 2020.
  - The 17th International Conference on Trust, Privacy and Security in Digital Business, 14-17 September 2020.
  - 15th International Workshop on Data Privacy Management. 17-18 September 2020.
  - 6th ACM Cyber-Physical System Security Workshop (ACM CPSS 2020) in conjunction with ACM Asia CCS'20. 6 October 2020.
- Dr. Liliana Pasquale (UCD) was program co-chair together with Nazim Madhavji of the 26th working conference on requirements engineering: Foundation for Software Quality (REFSQ 2020).

2.3.6 Presentations at Events

- TDL represented CyberSec4Europe in the meeting organised by cyberwatching.eu on “Lightweight synergies for projects with MTRL 5-7”.
- GUF delivered a talk on "CyberSec4Europe & Standardisation: Aiming to safeguard values through excellence in cybersecurity" to CyberSec4Europe WP 8 Webinar “Integrating an ecosystem perspective in cybersecurity standards”, December 2020.

- CNR participated in the ISTI Day organised by CNR in November 2020. In particular, they participated by presenting a poster entitled 'Data Protection Compliance Through Access Control' and delivered a series of talks on CyberSec4Europe.
- Dan Bogdanov (CYBER) was part of a panel discussion at the CPDP conference, Brussels, January 2020.
- GUF presented CyberSec4Europe's views on certification at ENISA's Cybersecurity Standardization Conference 2020, Athens, February 2020.
- GUF delivered a presentation at the 14th IFIP orking Group 11.10 International Conference on Critical Infrastructure Protection (ICCIP), held in Arlington, Virginia, March 2020.
- CyberSec4Europe presentation at the first faculty-wide internal research seminar of the Faculty of Economics and Business Administration at GUF, online, March 2020.
- GUF presented CyberSec4Europe and participated in a panel at the SEREN4 Horizon 2020 workshop, online, April 2020.
- GUF organised together with KDDI Research a workshop including a presentation on CyberSec4Europe, online, July 2020.
- GUF gave a presentation at 2nd Model-Driven Simulation and Training Environments for Cybersecurity (MSTEC), co-located with the The European Symposium on Research in Computer Security (ESORICS), online, September 2020.
- GUF co-presented at the 2nd Workshop on Security, Privacy, Organizations, and Systems Engineering (SPOSE), co-located with the The European Symposium on Research in Computer Security (ESORICS), online, September 2020.
- GUF gave a prsentation on "CyberSec4Europe – Aiming to safeguard values through excellence in cybersecurity" at IFIP Sec 2020, online, September 2020.
- GUF presented "CyberSec4Europe – Aiming to safeguard values through excellence in cybersecurity" at "Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz" German Federal States' Ministries of the Interior WG on cybersecurity, online, October 2020.
- Impulse Speech "Data Protection in the context of IoT" at 3rd German Japanese Security Forum, delivered by GUF, online, November 2020.
- UMU presented a paper related to challeges of security updates at the Global Summit conference, online, June 2020,
- UMU delivered an invited presentation on 'CyberSec4Europe roadmap' at the ECSO WG6 Meeting, online, December 2020.
- UCD presented a paper on "Automated modelling of security incidents to represent logging requirements" at the ARES conference, online, August 2020.
- Liliana Pasquale (UCD) delivered a presentation about her paper published 10 years ago titled "Fuzzy Goals for Requirements-Driven Adaptation", which received the Most Influential Paper Award at the RE 2020 conference.
- Bashar Nuseibeh (UCD) was a keynote speaker for Informatics Europe ECSS 2020 - the 16th European Computer Science Summit, online, 26-28 October 2020.
- UPRC presented "CyberSec4Europe Maritime Transport Risk Assessment Approach" in the 4th Cybersecurity Conference in Maritime Domain" of the NATO Maritime Interdiction Operational Training

Centre (NMIOTC). The conference was attended by Allied and Partner Nations, International Organizations the international academic community and representatives from the shipping and IT industry, online and in person, September 2020

- UPRC presented CyberSec4Europe goals and ambitions in the Cyberwatching.eu webinar on "Effective protection of Critical Infrastructures against cyber threats". The event was held online in October 2020.

2.3.7 Hackathons and Pitstops

BRNO organised several events of these types. We distinguish between a hackathon, as a single isolated event of any duration, and a pitstop, which is a shorter event (checkpoint) within a larger effort, generally a summer school.

- April-May 2020: students at Masaryk University created sandboxes deployed in the KYPO Cyber Range Platform, that were then used for a Hacking Day event. This event was a coordinated effort with CONCORDIA.
- Hackathon held in July 2020 within the KYPO Summer School for high school students. This event was a coordinated effort with CONCORDIA.
- In November 2020 students at Masaryk University completed training in a sandbox locally generated with the Cyber Sandbox Creator as a a pitstop.
- During December 2020 and January 2021 students at Masaryk University created sandboxes deployed in the KYPO Cyber Range Platform, that were then used for a Hacking Day event. This event was a coordinated effort with CONCORDIA.
- Pitstops: from October 2020 to April 2021 students at The Slovak University of Technology were creating sandboxes for their cybersecurity games as a team project.

2.4 Business

- UPS-IRIT delivered an invited talk at Rencontres Cybersécurité d'Occitanie, on “The future European regulation on Cybersecurity Competence Centres”, online, June 2020.
- David Goodman (TDL) gave an animated presentation of OBSIDIAN at the 'Cybersecurity in Finance' workshop, organised by the SOTER project, involving other finance-related H2020 projects including SOTER, Critical Chains, FIN-TECH, FINSEC, SPARTA and CONCORDIA, online, 30 October 2020.
- David Goodman (TDL) gave a presentation on 'Regulatory Disharmony and Disruptive Technologies in the Financial Sector' at the 'Financial Sector Infrastructure, Cyber-Physical Security and Regulatory Standards' workshop, organised by the Critical-Chains project, involving other finance-related H2020 projects including SOTER, Critical-Chains, CS-Aware, Poste Italiane, Caixa Bank, L-SEC and CONCORDIA, online, 14 December 2020.
- AIT presented the ambition and goals of CyberSec4Europe at the Austrian "Platform Industrie 4.0".
- ATOS participated in the conference "Towards the future of cybersecurity" organised by INCIBE, where they presented CyberSec4Europe, online, October 2020.
- GUF delivered a presentation "Assessing Privacy Protection & Data Transfer in Smart Systems" at the 4th World Conference on Smart Trends in Systems, Security and Sustainability (WS4 2020), online, July 2020.

- GUF and ATOS delivered a presentation on "CyberSec4Europe – Aiming to safeguard values through excellence in cybersecurity" at European Federation of Medical Informatics (EFMI) 2nd EU-China Health Summit MIMTT 2020, October 2020.
- GUF presented at the European Big Data Value Forum (EBDVF), Session "Privacy-preserving technologies - a key enabler of big data for AI" key results on CyberSec4Europe, November 2020.
- GUF participated in the panel "Cyber Security - Technology and Security in the Age of Pandemic" at International Digital Security Forum (IDSF), online, December 2020.
- KUL participated in the CyberSec & AI Connected 2020 event, online, October 2020.
- OASC participated in the events organised by ETSI, in particular, in the Industry Specification Group for the RGS/CIM-0009v131 standard.
- OASC participated in the Specialist Task Force of ETSI for the development of test for standard from ETSI ISG CIM.
- UM presented the project at the conference (INT 2019 – INFOSEC New Technologies), primarily aimed at industry in Slovenia held in Nova Gorica, Slovenia, June 2020.
- UPRC presented the CyberSec4Europe along with the maritime transport demonstrator use case at the Cypber event 2020. The attendees were mainly government advisors, IT security professionals, computer & informatics engineers professionals, delegates from shipping, ports, oil & gas, energy sector), decision makers, policy makers, legal counsel, risk analyst, compliance, service providers, suppliers, sub–contractors, researchers and academics.
- UPRC participated in the meeting on the working group for maritime transport at the meeting organized by ENISA on ‘ENISA Maritime Cybersecurity Project’. The project intended to provide a comprehensive stocktaking and mapping of the growing number of initiatives, regulations, standards, guidelines etc regarding the maritime sector. Furthermore, the working group developed a mapping of security controls of key identified standards (including at least the NIS Cooperation Group Security Measures for OES, ISO 27001, NIST, BIMCO guidelines) to the security measures proposed in the 2019 ENISA report.
- UPRC delivered network security and wireless security courses and curricula for industry, online, May 2020.
- UCD was part of a panel of business experts to discuss how cyber threat intelligence can help optimise incident response processes so that enterprises can respond faster and reduce adversary opportunity.
- ABI Lab, attended five meetings of the Cyber Knowledge and Security Awerness Observatory of CERTFn, during which the Constituency was updated on the progress of all European projects. These meetings were held virtually in March, April, July, October and December.
- ABI Lab presented the CERTFin and also reported on the European projects in which it participates, including CyberSec4Europe among them. The event was held in Brussels in February 2020.
- ABI Lab presented the CERTFin and the initiatives in which it is involved in an event held in February 2020 in Barcelona.

2.5 Governmental

- GUF participated in the DG CNECT H.1 workshop on "joint actions" with Member States, Brussels, February 2020.

- GUF had a metting with Katja Kümmel (Hessen Ministry of Economy) as part of the Mercator Science-Policy Fellowship Program, November 2020.
- GUF had a meeting with Felix Haas (STERN magazine) as part of the Mercator Science-Policy Fellowship Program, November 2020.
- UMA organised the event for the local authorities in Malaga on 'The importance of cybersecurity for Tourism. Aspects to tackle' online, July 2020.
- UMA participated in the XIV Day on Security, Defense and Cooperation organised by the Spanish Government, July 2020.
- TLEX gave a presentation on the Schrems II judgement of the European Court of Justice at a webinar organised by the Cybersecurity Coallition, online June 2020.
- TLEX moderated and participated in a roundtable webinar on the security of personal data organised by the European Incubator of the Brussels Bar, online, December 2020.

2.6 Standardisation

Even though listed here are some of the standards meetings partners attended, [D8.3] contains much more detail on these activities.

AIT participated in the following standardisation events:

- Remote participation in 69th ASI AG 001.27 meeting (Austrian mirror committee of ISO/IEC JTC1/SC27), Vienna, February 2020.
- Periodic ISO/IEC JTC1/SC27 ("Information security, cybersecurity and privacy protection") working group meetings. AIT participated as liaison officer for CyberSec4Europe to WG2, and as editor of multiple standards in WG2, online, 20-24 April 2020.
- Participation in the 70th ASI AG 001.27 meeting (Austrian mirror committee of ISO/IEC JTC1/SC27), online, May 2020.
- Participation in 71st ASI AG 001.27 meeting (Austrian mirror committee of ISO/IEC JTC1/SC27), online, September 2020.
- Periodic ISO/IEC JTC1/SC27 ("Information security, cybersecurity and privacy protection") working group meetings. AIT participated as liaison officer for CyberSec4Europe to WG2, and as editor of multiple standards in WG2, online, 12-16 September 2020.

ATOS contributed to the "NWIP Additional requirements for ISO/IEC 27701 – DRAFT", organised by the new study group for Feasibility study on European implementation of ISO/IEC 27701 depending of UNE, the Spanish Association for Standardisation ,

CYBER participated in the following standardisation meetings and activities as part of their membership in ISO/IEC working groups:

- JTC 1/SC 27 WG2
- JTC 1/SC 27 WG5

- EVS/TK 75 (Blockchain and distributed ledger technologies)
- EVS/TK 04 (Information technology)
- EVS/TK 75 (Blockchain and distributed ledger technologies)

GUF participated in the following meetings related to standardisation:

- DIN NIA 27 AA 'IT-Sicherheitsverfahren' (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs), Berlin, February 2020.
- DIN BR-07 (German Mirror Committee to CEN/CLC JTC 13 Cybersecurity and Data Protection), online, March 2020.
- ISO/PC 317 and ISO/PC 317/WG 1. 'Consumer protection: privacy by design for consumer goods and services', online, March and April 2020.
- CEN/CLC JTC 13 Cybersecurity and Data Protection and WGs, online, March 2020.
- ISO/IEC JTC 1/SC 27 WGs, especially WG 5 "Identity Management and Privacy Technologies", online, April 2020.
- Chair Advisory Group of ISO/IEC JTC 1/SC 27 "Information security, cybersecurity and privacy protection", online, May 2020.
- ISO/IEC JTC 1/SC 27 Conference "The Future of Standards in Cybersecurity", especially Stream III "Hot issues in cybersecurity", online, September 2020.

SIE participated in the following activities of different standardisation bodies:

- IEC 62443 of ISO.
- Collaborative Automated Course of Action Operations (CACAO), Cyber Threat Intelligence (CTI), Open Command and Control (OpenC2) working groups of OASIS.
- CSA STAR (Security Trust Assurance and Risk) and CSA CCM (Cloud Controls Matrix),
- Web of Things (WOT) part of the W3C.

UMU participated in the ETSI working group, ISG CIM: Industrial Specification Group Cross-cutting Information Management.

SINTEF has participated in the following standardisation activities:

- ISO/IEC (specifically JTC 1/SC 27 - IT Security techniques) and Standards Norway (SN/K 171 IT Sikkerhet)

UCD participated in the ISO/IEC working group on the revised IEC 80001-1, registered as a Draft International Standard (DIS) and that will be published later in 2021.

CyberSec4Europe, involving ARCH, CYBER and TDL, hosted the first two webinars in a new Insights series:

- Integrating an ecosystem perspective in cybersecurity standards, 18 December 2020

- Cybersecurity & Standards – How StandICT.eu supports European specialists in the international landscape, 29 January 2021

3 Achievement of KPI Indicators

[D9.3] identified the list of KPIs indicating the measures of success of CyberSec4Europe in relation to the activities listed above. This list is shown in Table 1 to which we have added the column of achievements up to January 2021. We describe next how the CyberSec4Europe partners have performed in relation to these KPI. Note that the timeline target of these KPIs is for the whole duration of the project, and these results reflect achievements after the first 24 months, including those from the first 12 months in a separate column. Hence these figures are an update of those shown in [D9.5].

Activity	KPI/Target	Achieved M13-M24	Achieved M01-M12
Flash studies, production of CyberSec4Europe leaflets	≥ 3, one per annum	As face-to-face meetings only took place during the first month of this review period, we did not produce any new leaflets.	9
Participation in 6 public exhibitions and demonstrations	3 per annum after M12	21	Already carried out, however it was expected after M12
Journal publications in international referred journals	More than 30	30	5
Reviewed publications/presentations in	More than 50	36	17
CyberSec4Europe co-organised workshops	More than 2 workshops, each attended by more than 40 participants, with more than 20 external toroject	9	7
CyberSec4Europe tutorials	More than 2 tutorials co-located with summer-schools, more than 1 in a relevant conference	1	
Organization and hosting of 4 hackathons / pitstops	To take place after M12	5	
6 presentations at meetups	2 per annum after M1	31 (including business and legislative events)	20

CyberSec4Europe newsletters through social media dissemination and news on website	6 newsletters with 1 issue/participation every 6 months	38 (See also [D9.9])	5

Table 1 Key Performance Indicator results up to M24

4 Joint Activities with the other Three Pilots

DG CONNECT has worked closely with the four pilots funded under the call SU-ICT-03-2018 call (CONCORDIA, ECHO, SPARTA, CyberSec4Europe) to show that, even though their work on cybersecurity topics varies, they share the common goal of piloting the Cybersecurity Competence Centre and Network.

GUF and TDL participated in the DG CONNECT organised (online) meetings together with JRC, REA, ECSO and the other pilot coordinators in September, November 2020 and January 2021.

With support from the other three pilot projects and the friendly support of the Representation of the State of Hessen to the EU, CyberSec4Europe organised CONVERGENCE: Making The European Cybersecurity Competence Network A Reality, held online from 9-11 December 2020. Each of the four pilots had their own session to present their activities and achievements and participated in six focus group sessions. The event was opened with an evening panel discussion featuring senior representatives from the three European Institutions (Parliament, Council and Commission) as well as the EDPS and moderated by David Goodman (TDL). Recordings of all the sessions are available on both websites (see also [D10.2]).

Most of the focus groups started up during 2020 (except for Communications which started in February 2019) and will continue through 2021, reporting to the bi-monthly co-ordinators' meetings. Regular updates will be posted to the CCN website.

- Communications Group:

  CyberSec4Europe, represented by TDL, held the chair of the four pilots' communications group from August 2020 to January 2021, during which time it ran five monthly (online) meetings, co-ordinated with DG CONNECT on participation in European Cybersecurity Month (October 2020), monthly contributions to the DG CONNECT Cybersecurity and Privacy newsletter and promoting and engaging with the JRC's Cybersecurity Atlas. TDL was responsible for managing and updating the CCN website and Twitter account, in particular ensuring that the CONVERGENCE event page was managed and updated daily on both the CCN and CyberSec4Europe websites. TDL published a six to nine month strategy plan for the communications group in July 2020, which it updated prior to handing over the rotating role of chair to CONCORDIA at the end of January 2021.

- Threat Intelligence Focus Group

  With CONCORDIA (chair) and CyberSec4Europe, the group met (online) in June 2020 and involved the participation of UMU, TDL and I-BP in subsequent activities.

- Roadmapping Focus Group

  Involving all four pilots and chaired by SPARTA, FORTH, GUF and TDL attended two (online) meetings of the group in September and November 2020.

- Education Focus Group

  UNITN attended the (online) meetings organised by ENISA and ECSO to discuss the future CCN education mapping in September and November 2020.

5 Conclusion

In this deliverable we have described the outreach activities carried out by CyberSec4Europe partners during the second year of the project. We have described these activities by following the target audiences identified in ([D9.3]).

We have referenced the KPIs that will determine the success of the project. These KPIs are related to the organisation of meetings, workshops, publications, the use of dissemination material or participation in summer schools. The analysis of these KPIs indicate that, after two years, the outreach activities are well in advance of the expected outcomes at this stage of the project.

A very important part of the dissemination activities comes under the umbrella of the four pilots' communications group, organised with the other three pilots. CyberSec4Europe plays a key role in this group.

6 References

[D8.3] Cybersecurity Standardization Engagement Plan 2

[D9.3]. Dissemination and Awareness Plan.

[D9.5] Report on the Outreach and Dissemination Activities I

[D9.7] CyberSec4Europe summer school,

[D9.9] Website and social media accounts 3

[D9.16] CyberSec4Europe summer school 2

[D10.2] Clustering Results and Concertation Conference Year 2