|  |  |
| --- | --- |
| Proposal No. 830929 | Project start: 1 February, 2019 |
| Call H2020-SU-ICT-03-2018 | Project duration: 47 months |



**D9.23**

**Final report on the outreach and dissemination activities**

|  |  |
| --- | --- |
| **Document Identification** | |
| Due date | 31 December 2022 |
| Submission date | 23 January 2023 |
| Revision | 1.1 |

|  |  |  |  |
| --- | --- | --- | --- |
| Related WP | WP9 | Dissemination Level | PU |
| Lead  Participant | UMA | Lead Author | Carmen Fernandez-  Gago (UMA) |
| Contributing Beneficiaries | TDL, UMA | Related Deliverables | D9.5, D9.10 |

i

**Abstract:** This document describes the dissemination and communication activities carried out by the CyberSec4Europe partners during the third period 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. This document and its content are the property of the CyberSec4Europe Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the CyberSec4Europe Consortium and are not to be disclosed externally without prior written consent from the CyberSec4Europe Partners. Each CyberSec4Europe Partner may use this document in conformity with the CyberSec4Europe Consortium Grant Agreement provisions and the Consortium Agreement.  The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. |  |

## Executive Summary

This report is the last in a series of three deliverables following the two previous reports, [D9.5] and [D9.10] which covered the first and second years of the proeject respectively. This report covers the outreach activities of all the consortium partners during the last two years of CyberSec4Europe and provides details of their dissemination and communication activities These activities follow the project's strategic plan for communication and dissemination as outline in [D9.3], and aligns with the classification of different target audiences and different dissemination and communication channels.

## Document information

### Contributors

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

**Reviewers**

|  |  |
| --- | --- |
| **Name** | **Partner** |
| Natalia Kadenko | TUD |
| Christine Jamieson | TDL |

**History**

|  |  |  |  |
| --- | --- | --- | --- |
| v0.1 | 2022-11-01 | Carmen Fernandez-Gago | Proposed table of contents and First draft |
| v0.2 | 2022-17-12 | Carmen Fernandez-Gago, Javier Lopez | First version sent for review |
| v1.0 | 2022-20-12 | Carmen Fernandez-Gago | Reviewers comments addressed |
| v1.0 | 2022-12-23 | Ahad Niknia | Final check, preparation and  submission process |
| v1.1 | 2023-01-12 | David Godman | Final version |
| V1.1 | 2023-01-23 | Ahad Niknia | Final check, preparation, and resubmission |

**List of Contents**

1. [Introduction 1](#_bookmark0)
2. [Dissemination and Outreach Activities 2](#_bookmark1)
   1. [Social 2](#_bookmark2)
   2. [Technical 2](#_bookmark3)
   3. [Scientific 3](#_bookmark4)
      1. [Articles in Journals 3](#_bookmark5)
      2. [Articles at Conferences 7](#_bookmark6)
      3. [Book Chapters 13](#_bookmark7)
      4. [Books 14](#_bookmark8)
      5. [PhD Thesis or MSc Thesis 14](#_bookmark9)
      6. [Summer Schools 14](#_bookmark10)
      7. [Organisation of Events (Conference and Workshops) 14](#_bookmark11)
      8. [Presentations at Events 16](#_bookmark12)
   4. [Business 19](#_bookmark13)
   5. [Governmental 21](#_bookmark14)
   6. [Standardisation 21](#_bookmark15)
3. [Achievement of KPI Indicators 23](#_bookmark16)
4. [Community Activities 24](#_bookmark18)
5. [Summary 25](#_bookmark19)
6. [References 26](#_bookmark20)

List of Tables

[Table 1 Key Performance Indicator results up to the end of the project 24](#_bookmark17)

**List of Acronyms**

AIT 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

# 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.

This deliverable is an update of [D9.10]. In this deliverable we follow 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 compare the achievements on dissemination and communication with the key performance indicators established in the strategy document as indicators of success and state that, for most of the KPIs. Despite the restrictions imposed by the pandemic, the dissemination activities were adapted in most cases to take place online. This means that CyberSec4Europe did not stop spreading the word, just as the technical work did not stop.

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 a summary of the deliverable.

# Dissemination and Outreach Activities

In this section we describe how the target audiences that we identified in [D9.3] were approached by the project partners during the last period of the project. Even though COVID-19 has had a continuing impact on face-to-face dissemination events, we all adapted to the situation and many events were carried out online or in a hybrid mode and even some events have come back to being in-person only events during 2022. We specify for each of these events the communication channel that was used.

## Social

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

* + - Press release on Momentum! published by TDL on 30th November 2022 through social media, mailing lists and an international press wire (EIN).
    - ATOS participated in an interview related to the underlying design decisions when building Data Spaces, conducted by ISST Fraunhofer, IDSA and the Chair of Industrial Information Management at TU Dortmund University, online, October 2022.
    - UMA delivered a talk at the Webinar#CyberHerTalk, Women4Cyber, September 2022.
    - UM participated as a guest on a national Slovenian television on the topic of cybersecurity, attacks and warfare, who the attackers are, the consequences of cyber attacks, and how to defend against them. May 2022.
    - UM participated as a guest on national Slovenian television on the topic of passwords (traps, how to build them etc.).
    - UM members were interviewed by Slovenian national television on two different topics in February 2021:
      * Safer internet day, mention of CyberSEc4Europe.
      * Interview on cybersecurity, mention of CyberSec4Europe.
    - GUF contributed to a publication of the European Parliament on “The European Digital Identity Wallet – a great opportunity & challenge at the same time”, March 2022.
    - GUF maintained a discussion with Dr. Petra Raderschall (Stiftung Warentest) as part of the Mercator Science-Policy Fellowship Program, June 2021, online.
    - UMU broadcasted on the topic of awareness for IoT (“La gente no es consciente de lo expuesta que está con el internet de las cosas”), BBVA Deeptalks podcasts (Bank initiative), December 2021.
    - UMU’s interview in El Pais (Spanish national newspaper) on awareness for IoT. November 2021

## Technical

* + - A regular series of lectures on Frankfurter Gespräche zum Informationsrecht (GUF).

## Scientific

All the publications listed below are open access through the project website.

### Articles in Journals

* + - * Sara Nieves Matheu Garcia, Enrique Mármol, Jose L. Hernandez-Ramos, Antonio Skarmeta, Gianmarco Baldini. *Federated cyberattack detection for IoT-enabled Smart Cities.* IEEE in Computer, vol. 55, no. 12, pp. 65-73, 2022, [doi: 10.1109/MC.2022.3195054](https://ieeexplore.ieee.org/abstract/document/9963740)
      * Daniele Bringhenti, Jalolliddin Yusupov, Alejandro Molina Zarca, Fulvio Valenza, Riccardo Sisto, Jorge Bernal Bernabe, Antonio Skarmeta. *AItomatic, verifiable and optimized policy-based security enforcement for SDN-aware IoT networks.* Computer Networks, vol. 213, Elsevier, 2022. <https://doi.org/10.1016/j.comnet.2022.109123>
      * Enrique Mármol Campos, Pablo Fernández Saura, Aurora González-Vidal, José L. Hernández- Ramos, Jorge Bernal Bernabe, Gianmarco Baldini, Antonio Skarmeta. *Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges.* Computer Networks, Volume 203, 108661, ELSEVIER, 2022. <https://doi.org/10.1016/j.comnet.2021.108661>
      * Luca Allodi, Fabio Massacci, Julian Williams. *The work*‐*averse cyberattacker model: theory and evidence from two million attack signatures.* Risk Analysis Journal, Volume 42(8), pp: 1623-1642. Wiley, 2022. <https://doi.org/10.1111/risa.13732>
      * Daniele Friolo, Fabio Massacci, Chan Nam Ngo, Daniele Venturi. *Cryptographic and Financial Fairness.* IEEE Transactions on Information Forensics and Security. Volume 17, 2022. Pp: 3391 – 3406, IEEE. [doi: 10.1109/TIFS.2022.3198852.](https://ieeexplore.ieee.org/document/9856685)
      * Bart Verkuil, Carlos E. Budde, Doina Bucur. *Automated fault tree learning from continuous-valued sensor data: a case study on domestic heaters*. International Journal of Prognostics and Health Management, Volume 13(2), 2022. PHM Society, <https://doi.org/10.36001/ijphm.2022.v13i2.3160>
      * Carlos E. Budde. *FIG: the Finite Improbability Generator v1.3.* ACM SIGMETRICS Performance Evaluation Review, Volume 49(4), 2022, pp: 59-64. <https://doi.org/10.1145/3543146.3543160>
      * Fabio Massacci and Silvia Vidor. *Building Principles for Lawful Cyber Lethal Autonomous Weapons.* IEEE Security & Privacy, Volume 20(2), 2022, pp: 101-106. [doi: 10.1109/MSEC.2022.3143269](https://ieeexplore.ieee.org/document/9740711).
      * Marko Hölbl, Boštjan Kežmah, Marko Kompara. *Data Protection Heterogeneity in the European Union.* Applied Sciences. 2021, 11(22), 10912; <https://doi.org/10.3390/app112210912>
      * Lili Nemec Zlatolas, Luka Hrgarek, Tatjana Welzer and Marko Hölbl. *Models of Privacy and Disclosure on Social Networking Sites: A Systematic Literature Review.* Mathematics 2022, 10(1), 146; MDPI. <https://doi.org/10.3390/math10010146>
      * Sunil Chaudhary, Vasileios Gkioulos, Sokratis Katsikas. *Developing metrics to assess the effectiveness of cybersecurity awareness program.* Journal of Cybersecurity. Volume 8, Issue 1, 2022, Oxford Academy, 2022. <https://doi.org/10.1093/cybsec/tyac006>
      * André Cirne Patrícia R.Sousa João S.Resende Luís Antunes. *IoT security certifications: Challenges and potential approaches.* Computers & Security, Volume 116, May 2022, 102669. Elsevier, 2022. <https://doi.org/10.1016/j.cose.2022.102669>
      * Inês Martins, João S.Resende, Patrícia R.Sousa, Simão Silva, Luís Antunes, João Gama*. Host-based IDS: A review and open issues of an anomaly detection system in IoT.* Future Generation Computer

Systems, Volume 133, August 2022, Pages 95-113. Elsevier 2022. <https://doi.org/10.1016/j.future.2022.03.001>

* + - * Carmine Caserio,Francesca Lonetti and Eda Marchetti*. A Formal Validation Approach for XACML*

*3.0 Access Control Policy.* Sensors 22(8), pp: 1424-8220, MDPI 2022 <https://doi.org/10.3390/s22082984>

* + - * Panagiotis Bountakas, Christoforos Ntantogian, Christos Xenakis. *EKnad: Exploit Kits’ network activity detection*. Future Generation Computer Systems Vol.134, pp:219-234, Elsevier, 2022 10.1016/j.future.2022.04.001
      * Mohammad Shahraeini, Panayiotis Kotzanikolaou and Mehrab Nasrolahi. *Communication Resilience for Smart Grids Based on Dependence Graphs and Eigenspectral Analysis, IEEE Systems JournalEarly access article, IEEE, 2022* <https://doi.org/10.1109/JSYST.2022.3179660>
      * Christos Grigoriadis, Romain Laborde, Antonin Verdier, and Panayiotis Kotzanikolaou. *An Adaptive, Situation-Based Risk Assessment and Security Enforcement Framework for the Maritime Sector,* Sensors*,* Vol. 22, no. 1:238, pp: 25464-25493, MDPI, 2022. <https://doi.org/10.3390/s22010238>
      * Casino, Fran, Thomas K. Dasaklis, George Spathoulas, Marios Anagnostopoulos, Amrita Ghosal, Istvan Borocz, Agusti Solanas, Mauro Conti, and Constantinos Patsakis, *Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews*, IEEE Access, Vol.10, I[EEE 2022. 10.1109/ACCESS.2022.3154059](https://doi.org/10.1109/ACCESS.2022.3154059)
      * Vasilis Vouvoutsis, Fran Casino, Constantinos Patsakis. *On the Effectiveness of Binary Emulation in Malware Classification*. Journal of Information Security and Applications, arXiv:2204.04084, Elsevier, 2022. 10.1016/j.jisa.2022.103258
      * Fran Casino, Nikolaos Totosis, Theodoros Apostolopoulos, Nikolaos Lykousas, Constantinos Patsakis. *Analysis and Correlation of Visual Evidence in Campaigns of Malicious Office Documents*. Digital Threats: Research and Practice, ACM, 2022 10.1145/3513025
      * Evangelos Mantas, Constantinos Patsakis. *Who watches the new watchmen? The challenges for drone digital forensics investigations*, Array, Vol. 14 (100135), Elsevier, 2022. 10.1016/j.array.2022.100135
      * Hoffmann, J.; Müllmann, D. *Das Standardsetzungsmodell des IT-Sicherheitsrechts im Kontext kritischer Infrastrukturen.* Die Verwaltung. Number 4, 2022. Duncker & Humblot GmbH, Berlin.
      * V Liagkou, P. Nastou, P. Spirakis, Y. Stamatiou. How Hard Is It to Detect Surveillance? A Formal Study of Panopticons and Their Detectability Problem. Cryptography 6.3 (2022): 42. MDPI. <https://doi.org/10.3390/cryptography6030042>
      * R. Rios, J. A. Onieva, R. Roman, and J. Lopez. *Personal IoT Privacy Control at the Edge.* IEEE Security & Privacy, vol 20, issue 1, IEEE,, 2022. Pp:23-32, [10.1109/MSEC.2021.3101865](https://ieeexplore.ieee.org/document/9516686)
      * von Wintzingerode, C.; Müllmann, D.; Spiecker gen. Döhmann, I. *Ein Netzwerk für Europas Cybersicherheit,* Neue Zeitschrift für Verwaltungsrecht (NVwZ). Number 10, pp. 690-695, 2021.
      * Paolo Barsocchi Antonello Calabrò Antonino Crivello Said Daoudagh Francesco Furfari Michele Girolami Eda Marchetti. *COVID-19 & privacy: Enhancing of indoor localization architectures towards effective social distancing*. Array, Volume 9, 2021, 100051, Elsevier. <https://doi.org/10.1016/j.array.2020.100051>
      * Panagiotis Gkotsiopoulos, Dimitrios Zorbas, Christos Douligeris. *Performance Determinants in LoRa Networks: a Literature Review.* ΙΕΕΕ Communications Surveys & Tutorials, Vol.23(3) thirdquarter 2021, 1721-1758, 1553-877X IEEE 2021. 10.1109/COMST.2021.3090409
      * Stylianos Karagiannis, Christoforos Ntantogian, Emmanouil Magkos, Luís L. Ribeiro, Luís Campos. *PocketCTF: A Fully Featured Approach for Hosting Portable Attack and Defense Cybersecurity Exercises*. Information Journal, Vol. 12(8), pp: 2078-2489, MDPI, 2021. <https://doi.org/10.3390/info12080318>
      * Fran Casino, Nikolaos Lykousas, Ivan Homoliak, Constantinos Patsakis, and Julio Hernandez- Castro *Intercepting Hail Hydra: Real-time detection of Algorithmically Generated Domains*, Journal of Information Security and Applications, vol. 190. Elsevier 2021. <https://doi.org/10.1016/j.jnca.2021.103135>
      * F. Casino, N. Lykousas, V. Katos, C Patsakis. *Unearthing malicious campaigns and actors from the blockchain DNS ecosystem*, Computer Communications, vol 179(1). Elsevier, 2021. 10.1016/j.comcom.2021.08.023
      * Vasilios Koutsokostas, Nikolaos Lykousas, Theodoros Apostolopoulos, Gabriele Orazi, Amrita Ghosal, Fran Casino, Mauro Conti, Constantinos Patsakis. *Invoice #31415 attached: Automated analysis of malicious Microsoft Office documents*. Computers & Security, vol. 114 Issue C, 2021.<https://doi.org/10.1016/j.cose.2021.102582>
      * Tsantilis, T.K. Dasaklis, C. Douligeris, C. Patsakis. *Searching Deterministic Chaotic Properties in System-Wide Vulnerability Datasets*. Informatics 2021, **8**(4)86; <https://doi.org/10.3390/informatics8040086>
      * G. Karantzas, C. Patsakis. An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors. Journal of Cybersecurity and Privacy, 1(3), 387- 421; 2021. 10.3390/jcp1030021
      * Vasilios Koutsokostas; Nikolaos Lykousas; Gabriele Orazi; Theodoros Apostolopoulos; Amrita Ghosal; Fran Casino; Mauro Conti, Constantinos Patsakis. *ManMalicious MS Office documents datasetdatory field.* Zenodo publications 2021. <http://doi.org/10.5281/zenodo.4559436>
      * Constantinos Patsakis and Fran Casino. *Exploiting statistical and structural features for the detection of domain generation algorithms.* Journal of Information Security and Applications. Volume 58 (102725), pp: 1-12. Elsevier, ScienceDirect 2021. 10.1016/j.jisa.2020.102725
      * Theodoros Apostolopoulos, Vasilios Katos, Kim-Kwang Raymond Choo, Constantinos Patsakis.*Resurrecting anti-virtualization and anti-debugging: Unhooking your hooks*. Future Generation Computer Systems, Vol. 116, pp: 393-40. Elsevier, 2021. 10.1016/j.future.2020.11.004
      * Said Daoudagh, Eda Marchetti, Vincenzo Savarino, Jorge Bernal Bernabé, Jesús García Rodríguez, Rafael Torres Moreno, Juan Antonio Martínez, Antonio F. Skarmeta. *Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal*. Sensors, vol 21 n. 21, MDPI, 2021. <https://doi.org/10.3390/s21217154>
      * Francesco Folino, Gianluigi Folino, Massimo Guarascio, Francesco Sergio Pisani, Luigi Pontieri. *On learning effective ensembles of deep neural networks for intrusion detection*. Information Fusion, Volume 72, August 2021, pp: 48-69, Elsevier, Netherlands, 2021. <https://doi.org/10.1016/j.inffus.2021.02.007>
      * Luca Durante, Lucia Seno, Adriano Valenzano. *A Formal Model and Technique to Redistribute the Packet Filtering Load in Multiple Firewall Networks.* IEEE Transactions on Information Forensics and Security, pp: 1—15, USA, 2021. <https://doi.org/10.1109/TIFS.2021.3057552>
      * Per Håkon Meland, Shukun Tokas, Gencer Erdogan, Karin Bernsmed, and Aida Omerovic. *A Systematic Mapping Study on Cyber Security Indicator Data.* Electronics, vol. 10, no. 9. MDPI, Basel (Switzerland), 2021. <https://doi.org/10.3390/electronics10091092>
      * V. Liagkou , P.E. Nastou, P. Spirakis2,, and Y.C. Stamatiou. *Effective enumeration of infinitely many programs that evade Formal Malware Analysis.* 5th International Symposium on Cyber Security Cryptology and Machine Learning (CSCML 2021), pp: 230-243.
      * J. Lopez, J. E. Rubio, and C. Alcaraz. *Digital Twins for Intelligent Authorization in the B5G- enabled Smart Grid.* IEEE Wireless Communications, vol. 28, issue 2, pp: 48-55. IEEE, 2021. 10.1109/MWC.001.2000336
      * S. Fischer-Hübner, C. Alcaraz, A. Ferreira, C. Fernandez-Gago, J. Lopez, E. Markatos, L. Islami, and M. Akil. *Stakeholder Perspectives and Requirements on Cybersecurity in Europe.* Journal of Information Security and Applications, 61 (102916), pp: 2214-2126, IEEE, 2021. 10.1016/j.jisa.2021.102916
      * Jorge Bernal Bernabé, Jesús García Rodríguez, Stephan Krenn, Vasia Liagkou, Antonio F. Skarmeta, Rafael Torres. *Privacy-Preserving Identity Management and Applications to Academic Degree Verification.* Privacy and Identity Management 2021, Online. Springer, (IFIP AICT,volume 644), pp: 33-46. [10.1007/978-3-030-99100-5\_4](https://link.springer.com/chapter/10.1007/978-3-030-99100-5_4)
      * Tobias Fiebig, Seda Gürses, Carlos H. Gañán, Erna Kotkamp, Fernando Kuipers, Martina Lindorfer, Menghua Prisse, Taritha Sari. *Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds.* arXiv, abs/2104-09462, 2021. <https://doi.org/10.48550/arXiv.2104.09462>
      * Alireza Esfahani, Jérémie Decouchant, Marcus Völp, Shahid Mumtaz, Kostromitin Konstantin Igorevich. SI-AKAV: *Secure integrated authentication and key agreement for cellular-connected IoT devices in vehicular social networks.* Transactions on Emerging Telecommunications Technologies. <https://doi.org/10.1002/ett.4279>
      * Patrícia R. Sousa Luís Magalhães João S. Resende Rolando Martins and Luís Antunes. *Provisioning, Authentication and Secure Communications for IoT Devices on FIWARE.* Sensors, 21(17), 5898. MDPI, 2021. <https://doi.org/10.3390/s21175898>
      * João S. Resende, Luís Magalhães, André Brandão, Rolando Martins and Luís Antunes. *Towards a Modular On-Premise Approach for Data Sharing.* Sensors 21(17), 5805, 2021. MDPI. <https://doi.org/10.3390/s21175805>
      * Tânia Carvalho ,Pedro Faria,Luís Antunes,Nuno Moniz. *Fundamental privacy rights in a pandemic state.* PLoS ONE 16(6): e0252169. <https://doi.org/10.1371/journal.pone.0252169>
      * André Brandao Joao S. Resende Rolando Martins. *Hardening of cryptographic operations through the use of Secure Enclaves.* Computers & Security, vol. 108, 102327, 2021. Elsevier. <https://doi.org/10.1016/j.cose.2021.102327>
      * Patrick Murmann, Matthias Beckerle, Simone Fischer-Hübner, Delphine Reinhardt. *Reconciling the what, when and how of privacy notifications in fitness tracking scenarios.* Pervasive and Mobile Computing, Volume 77, 2021, 101480. <https://doi.org/10.1016/j.pmcj.2021.101480>
      * Michalis Papaevripides and Elias Athanasopoulos. *Exploiting Mixed Binaries.* ACM Transactions on Privacy and Security,Volume 24, Issue 2, 2021. Article No.: 7, pp 1–29. <https://doi.org/10.1145/3418898>
      * Ganbayar Uuganbayar, Artsiom Yautsiukhin, Fabio Martinelli, Fabio Massacci. *Optimisation of cyber insurance coverage with selection of cost effective security controls.* Journal of Computers& Security, Volume 101, February 2021, 102121. 10.1016/j.cose.2020.102121
      * N. Dragoni, A. Lluch Lafuente, F. Massacci, A. Schlichtkrull. *Are we preparing students to build security in? A survey of european cybersecurity in higher education programs.* IEEE Computer and Reliability Societies. vol. 19, no. 1, pp. 81-88, 2021, 10.1109/MSEC.2020.3037446
      * Fabio Massacci, Trent Jaeger, Sean Peisert. *SolarWinds and the Challenges of Patching: Can We Ever Stop Dancing With the Devil?* in IEEE Security & Privacy, vol. 19, no. 2, pp. 14-19, 2021, [doi: 10.1109/MSEC.2021.3050433.](https://ieeexplore.ieee.org/document/9382358)
      * Fabio Massacci and Ivan Pashchenko. *Technical Leverage: dependencies mixed blessing.* IEEE Security & Privacy, vol. 19, no. 3, pp. 58-62, 2021, [10.1109/MSEC.2021.3065627](https://ieeexplore.ieee.org/document/9432442).
      * Ostrak, A., Randmets, J., Sokk, V., Laur, S., Kamm, L. *Implementing Privacy-Preserving Genotype Analysis with Consideration for Population Stratification.* Cryptography 2021, 5(3), 21; [https://doi.org/10.3390/cryptography5030021](https://www.mdpi.com/2410-387X/5/3/21)
      * Daoudagh, S.; Marchetti, E.; Savarino, V.; Bernabe, J.B.; García-Rodríguez, J.; Moreno, R.T.; Martinez, J.A.; Skarmeta, A.F. *Data Protection by Design in the Context of Smart Cities:* A Consent and Access Control Proposal. Sensors, vol 21, 7154. MDPI[, 2021. 10.3390/s21217154](https://www.mdpi.com/1424-8220/21/21/7154)
      * Jose L. Hernandez-Ramos, Sara N. Matheu, Angelo Feraudo, Gianmarco Baldini, Jorge Bernal Bernabe, Poonam Yadav, Antonio Skarmeta y Paolo Bellavista. *Defining the behavior of IoT devices through the MUD standard: review, challenges and research directions.* IEEE Access, vol.9, pp.12625-126285. doi: 10.1109/ACCESS.2021.3111477
      * Jose L. Hernandez-Ramos, Sara N. Matheu and Antonio Skarmeta. *The Challenges of Software Cybersecurity Certification.* IEEE Security & Privacy, vol. 19, no. 1, 2021. [10.1109/MSEC.2020.3037845](https://ieeexplore.ieee.org/document/9336084)
      * Oussama Tounekti, Antonio Ruiz-Martínez and Antonio F. Skarmeta-Gómez. *Users’ Evaluation of a New Web Browser Payment Interface for Facilitating the Use of Multiple Payment Systems.* Sustainability, 2021, 13(9), 4711, <https://doi.org/10.3390/su13094711>
      * Harborth, D. and Pape, S., *Investigating Privacy Concerns Related to Mobile Augmented Reality Apps - A Vignette Based Online Experiment*, Computers in Human Behaviour, vol 122, September 2021, http://dx.doi.org/10.1016/j.chb.2021.106833
      * Schmitz, C.; Schmid, M.; Harborth, D. and Pape, S., *Maturity Level Assessments of Information Security Controls: An Empirical Analysis of Practitioners' Assessment Capabilities*, Computers & Security, vol. 108 September 2021, http://dx.doi.org/10.1016/j.cose.2021.102306
      * Pape, S. and Kipker, D-K., *Case Study: Checking a Serious Security-Awareness Game for its Legal Adequacy*, [Datenschutz und Datensicherheit - DuD](https://www.springerprofessional.de/en/datenschutz-und-datensicherheit-dud/5316662)| [Issue 5/2021](https://www.springerprofessional.de/en/datenschutz-und-datensicherheit-dud-5-2021/19120150), http://dx.doi.org/10.1007/s11623-021-1440-3

### Articles at Conferences

* + - * Hien Truong, José L. Hernández-Ramos, Juan A. Martinez, Jorge Bernal Bernabe, Wenting Li, Agustin Marin Frutos, Antonio Skarmeta. *Enabling Decentralized and Auditable Access Control for IoT through Blockchain and Smart Contracts.* Security and Communication Networks, vol. 2022, Article ID 1828747, Hindawi, 2022. <https://doi.org/10.1155/2022/1828747>
      * Bernabe, J.B., García-Rodríguez, J., Krenn, S., Liagkou, V., Skarmeta, A., Torres, R. *Privacy- Preserving Identity Management and Applications to Academic Degree Verification.* IFIP Advances in Information and Communication Technology. Privacy and Identity Management. Between Data Protection and Security pp: 33–46, vol 644. Springer, Cham. [10.1007/978-3-030- 99100-5\_4](https://link.springer.com/chapter/10.1007/978-3-030-99100-5_4)
      * Pankova, Alisa; Laud, Peeter. *Interpreting Epsilon of Differential Privacy in Terms of Advantage in Guessing or Approximating Sensitive Attributes.* Proceedings of IEEE 35th Computer Security Foundations Symposium (CSF), pp: 96-111, IEEE Computer Society. [https://doi.org/10.1109/CSF54842.2022.00007](https://www.computer.org/csdl/proceedings-article/csf/2022/841700a096/1F9Ql5GVBZK)
      * Carlos E. Budde, Duncan Jansen, Inka Locht, and Mariëlle Stoelinga. *Learning to Learn HVAC Failures: Layering ML Experiments in the Absence of Ground Truth.* International Conference on Reliability, Safety, and Security of Railway Systems (RSSRail'22), volume 13294, Springer, 2022. [10.1007/978-3-031-05814-1\_7](https://link.springer.com/chapter/10.1007/978-3-031-05814-1_7)
      * Silvia Vidor and Carlos E. Budde. *A Maturity Assessment Model for Cyber Security Education in Europe.* IFIP World Conference on Information Security Education (WISE 22), vol. 650, Springer, pp:60-74. [10.1007/978-3-031-08172-9\_5](https://link.springer.com/chapter/10.1007/978-3-031-08172-9_5)
      * George Pantelakis, Panagiotis Papadopoulos, Nicolas Kourtellis & Evangelos P. Markatos. *Measuring the (Over)use of Service Workers for In-Page Push Advertising Purposes.* Passive and Active Measurement: 23rd International Conference, PAM 2022, Virtual Event, March 2022, pp: 426–438. <https://doi.org/10.1007/978-3-030-98785-5_19>
      * Panagiotis Papadopoulos Michalis Pachilakis Antonios A. Chariton Evangelos P. Markatos. *OUTOPIA: private user discovery on the internet.* EuroSec '22: Proceedings of the 15th European Workshop on Systems Security. 2022, Pages 8–14. <https://doi.org/10.1145/3517208.3523756>
      * Eva Anastasiadi, Elias Athanasopoulos, Evangelos Markats. *The Weakest Link: On Breaking the Association between Usernames and Passwords in Authentication Systems.* Proceedings of the 19th International Conference on Security and Cryptography - Volume 1: SECRYPT, ScitePress, 2021. 10.5220/0011276900003283
      * M. Gkolemi, P. Papadopoulos, E. Markatos, N. Kourtellis. *YouTubers Not madeForKids: Detecting Channels Sharing Inappropriate Videos Targeting Children.* WebSci '22: 14th ACM Web Science Conference 2022, pp: 370–381. <https://doi.org/10.1145/3501247.3531556>
      * M. Papadogiannakis, P. Papadopoulos, E. Markatos, N. Kourtellis. *Leveraging Google’s Publisher- Specific IDs to Detect Website Administration.* WWW '22: Proceedings of the ACM Web Conference 2022, pp: 2522–2531. <https://doi.org/10.1145/3485447.3512124>
      * Davy Preuveneers, Sander Joos and Wouter Joosen. *AuthGuide: Analyzing Security, Privacy and Usability Trade-Offs in Multi-factor Authentication.* Trust, Privacy and Security in Digital Business

- 18th International Conference, TrustBus 2021, Virtual Event, September 27-30, 2021, Proceedings. Lecture Notes in Computer Science 12927, [10.1007/978-3-030-86586-3\_11](https://link.springer.com/chapter/10.1007/978-3-030-86586-3_11)

* + - * Davy Preuveneers and Wouter Joosen. *Privacy-Preserving Polyglot Sharing and Analysis of Confidential Cyber Threat Intelligence.* ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security, 2022. Article No.: 2, pp: 1–11. <https://doi.org/10.1145/3538969.3538982>
      * Antreas Dionysiou and Elias Athanasopoulos. *Lethe: Practical Data Breach Detection with Zero Persistent Secret State.* 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P), 2022, pp. 223-235, 10.1109/EuroSP53844.2022.00022
      * Sunil Chaudhary, Marko Kompara, Sebastian Pape, Vasileios Gkioulos. *Properties for Cybersecurity Awareness Posters’ Design and Quality Assessment.* ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security. August 2022 Article 79, pp: 1–8. <https://doi.org/10.1145/3538969.3543794>
      * Sunil Chaudhary, Vasileios Gkioulos, and David Goodman. *Cybersecurity Awareness for Small and Medium-Sized Enterprises (SMEs): Availability and Scope of Free and Inexpensive Awareness Resources.* 8th Workshop On The Security Of Industrial Control Systems & Of Cyber-Physical Systems (CyberICPS 2022), Springer, Copenhagen, September 2022. In Press.
      * Simão Silva, Patrícia R. Sousa, João S. Resende & Luís Antunes. *Threat Detection and Mitigation with Honeypots: A Modular Approach for IoT.* 19th International Conference on Trust, Privacy and Security in Digital Business, TRUSTBUS 2022, Part of the Lecture Notes in Computer Science book series (LNCS,volume 13582), pp:66-80. Springer. Vienna. <https://doi.org/10.1007/978-3-031-17926-6_5>
      * B. Hofmann, P. Kasinathan and M. Wimmer. *Towards achieving confidentiality in Hyperledger Fabric.* 2022 IEEE International Conference on Blockchain (Blockchain) pp: 384-391. [10.1109/Blockchain55522.2022.00060](https://ieeexplore.ieee.org/document/9881834)
      * Abida Haque, Stephan Krenn, Daniel Slamanig, Christoph Striecks. *Logarithmic-Size (Linkable) Threshold Ring Signatures in the Plain Model.* Public-Key Cryptography - PKC2022, 2022, pp: 437-467, Springer, LNSC,volume 13178. [10.1007/978-3-030-97131-1\_15](https://link.springer.com/chapter/10.1007/978-3-030-97131-1_15)
      * Thomas Lorünser, Florian Wohner, Stephan Krenn. *A Privacy-Preserving Auction Platform with Public Verifiability for Smart Manufacturing.* International Conference on Information Systems Security and Privacy - ICISSP 2022, pp: 637-647, online. SCITEPRESS. [10.5220/0011006700003120](https://www.scitepress.org/Papers/2022/110067/110067.pdf)
      * Thomas Lorünser, Florian Wohner, Stephan Krenn. *A Verifiable Multiparty Computation Solver for the Linear Assignment Problem And Applications to Air Traffic Management.* ACM Cloud Computing Security Workshop - CCSW 2022, Los Angeles, <https://doi.org/10.1145/3560810.3564263>
      * Shukun Tokas, Gencer Erdogan, Ketil Stølen. *Privacy-aware IoT: State-of-the-art and challenges.* Proceedings of the 9th International Conference on Information Systems Security and Privacy 2023 (ICISSP'23), to appear February 2023.
      * Said Daoudagh, Eda Marchetti, Antonello Calabrò, Filipa Ferrada, Ana Inês Oliveira, José Barata, Ricardo Peres and Francisco Marques*. An Ontology-Based Solution for Monitoring IoT Cybersecurity.* 5th IFIP International INTERNET OF THINGS (IOT) Conference. pp: 158—176, Amsterdam, 2022. <https://doi.org/10.1007/978-3-031-18872-5_10>
      * Lucia Seno, Manuel Cheminod, Ivan Cibrario Bertolotti, Luca Durante, Adriano Valenzano. *Improving performance and cyber-attack resilience in multi-firewall industrial networks*, IEEE 18th International Conference on Factory Communication Systems (WFCS), April 2022 , pp: 1-8. Pavia, 2022. <https://doi.org/10.1109/WFCS53837.2022.9779199>
      * Massimo Guarascio, Marco Zuppelli, Nunziato Cassavia, Giuseppe Manco, Luca Caviglione. *Detection of Network Covert Channels in IoT Ecosystems Using Machine Learning.* ITASEC 2022. CEUR-WS.org, Rome. [http://star.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol- 3260/paper7.pdf](http://star.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-3260/paper7.pdf)
      * Said Daoudagh, Eda Marchetti. *The GDPR Compliance and Access Control Systems: Challenges and Research Opportunities.* Proceedings of the 8th International Conference on Information Systems Security and Privacy – ICISSP, SciTePress. Online Streaming, 2022.

<https://doi.org/10.5220/0010912300003120>

* + - * Vassilis Papaspirou, Maria Papathanasaki, Leandros Maglaras, Ioanna Kantzavelou, Christos Douligeris, Mohamed Amine Ferrag and Helge Janicke. *Security Revisited: Honeytokens meet Google Authenticator,* 7th SEEDA-CECNSM Conference, v1, pp: 1-6, SEEDA-CECNSM Conference, 2022. " <https://doi.org/10.48550/arXiv.2112.08431>
      * D. Koutras, C. Grigoriadis, M. Papadopoullos, P. Kotzanikolaou and C. Douligeris. *Automating environmental vulnerability analysis for network services* 10.1109/ISCC55528.2022.9912946. ISCC 2022 IEEE Symposium on Computers and Communications (ISCC), pp. 1-7. <http://doi.org/10.1109/ISCC55528.2022.9912946>
      * Christos Tselikis, Christos Douligeris, Sarandis Mitropoulos, Leandros Maglaras. *Re-Configuration from the Edge: Alternative Software Models for Time-Sensitive IoT Applications*, 2022 IEEE Symposium on Computers and Communications (ISCC) . [10.1109/ISCC55528.2022.9912979](http://doi.org/10.1109/ISCC55528.2022.9912979)
      * V Liagkou, P. Nastou, P. Spirakis, Y. Stamatiou. *On the undecidability of the Panopticon detection problem.* International Symposium on Cyber Security, Cryptology, and Machine Learning. CSCML 2022: Cyber Security, Cryptology, and Machine Learning pp 78–87. Lecture Notes in Computer Science book series (LNCS,volume 13301), Springer. [10.1007/978-3-031-07689-3\_6](https://link.springer.com/chapter/10.1007/978-3-031-07689-3_6)
      * Jack Edwards, Francisco J. Aparicio-Navarro, Leandros Maglaras, Christos Douligeris. *FFDA: A novel Four-Factor Distributed Authentication mechanism*. 2022 IEEE International Conference on Cyber Security and Resilience (CSR): Workshop on Maritime Cyber Security (MCS), pp:376- 381, ISBN: 978-1-6654-9952-1. 10.1109/CSR54599.2022.9850279
      * V. Liagkou, S. Sakka and C. Stylios. *Security and Privacy Vulnerabilities in Human Activity Recognition systems.* 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), held online in January 2022. IEEE. [doi: 10.1109/SEEDA-CECNSM57760.2022.9932957](https://ieeexplore.ieee.org/document/9932957).
      * Ioannis Kalderemidis, Aristeidis Farao, Panagiotis Bountakas, Sakshyam Panda, and Christos Xenakis. *GTM: Game Theoretic Methodology for optimal cybersecurity defending strategies and investments*. The 17th International Conference on Availability, Reliability and Security Art. No 120, pp: 1-9, ACM, ARES Conference, 2022. 10.1145/3538969.3544431
      * V. Liagkou, C. Stylios, L. Pappa, A. Petunin. *Challenges and opportunities in industry 4.0 for mechatronics, artificial intelligence and cybernetics.* Challenges and opportunities in industry 4.0 for mechatronics, artificial intelligence and cybernetics. Electronics 10.16. MDPI, 2022. <https://doi.org/10.3390/electronics10162001>
      * Said Daoudagh, Eda Marchetti. *GROOT: A GDPR-based Combinatorial Testing Approach*. The 33rd IFIP International Conference on Testing Software and Systems 2021. Lecture Notes in Computer Science 13045, pp: 210 - 217. Online Conference. [https://doi.org/10.1007/978-3-031- 04673-5\_17](https://doi.org/10.1007/978-3-031-04673-5_17)
      * Liagkou, Vasia, Antonio Skarmeta, and Rafael Torres. *Privacy-Preserving Identity Management and Applications to Academic Degree Verification.* Privacy and Identity Management. Between Data Protection and Security. Privacy and Identity 2021. IFIP Advances in Information and Communication Technology, vol 644. Springer, online 2022. [https://doi.org/10.1007/978-3-030- 99100-5\_4](https://doi.org/10.1007/978-3-030-99100-5_4)
      * D. Ferraris, C. Fernandez-Gago, and J. Lopez. *Verification and Validation Methods for a Trust-by- Design Framework for the IoT.* 36th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'22), Lecture Notes in Computer Science book series (LNCS),volume 13383, pp: 183-194, Newark (US), 10.1007/978-3-031-10684-2\_11
      * V. Liagkou , P.E. Nastou, P. Spirakis2,, and Y.C. Stamatiou. *Effective enumeration of infinitely many programs that evade Formal Malware Analysis.* 5th International Symposium on Cyber Security Cryptology and Machine Learning (CSCML 2021). Pp: 230-243, 2021. Springer online 2021. <https://doi.org/10.1007/978-3-030-78086-9_18>
      * Célia Martinie, Christos Grigoriadis, Eleni-Maria Kalogeraki, and Panayiotis Kotzanikolaou. *Modelling Human Tasks to Enhance Threat Identification in Critical Maritime Systems.* In Proceedings of the 25th Pan-Hellenic Conference on Informatics (PCI 2021), pp: 375-380. ACM, Volos, 2021. <https://doi.org/10.1145/3503823.3503892>
      * Christos Douligeris, Christos Grigoriadis. *Initial Results from the CyberSec4Europe*. 10th NMIOTC Annual Conference "Countering Hybrid Treats: An Emerging Maritime Security Challenge, 2021(2) 18-19, 2241-438X, 5th NMIOTC Cybersecurity Conference in Maritime Domain, 2021.
      * Ioannis Stellios, Kostas Mokos and Panayiotis Kotzanikolaou. *Assessing Vulnerabilities and IoT- Enabled Attacks on Smart Lighting Systems*. Within ESORICS 2021, International Workshops: CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP, and CDT&SECOMANE, Darmstadt, October 4–8, 2021, Revised Selected Papers (pp. 23-39). LNCS Vol. 13106, Springer, Darmstadt, 2021. <https://doi.org/10.1007/978-3-030-95484-0_2>
      * Athanasios Vasileios Grammatopoulos, Ilias Politis, Christos Xenakis. *A web tool for analyzing FIDO2/WebAuthn Requests and Responses*. The 16th International Conference on Availability, Reliability and Security, Art. No 125, pp: 1-10, ACM ARES Conference, 2021. 10.1145/3465481.3469209
      * Panagiotis Bountakas, Konstantinos Koutroumpouchos, Christos Xenakis. *A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection*. The 16th International Conference on Availability, Reliability and Security. Art. No 127, pp: 1-12, ACM, ARES Conference, 2021. 10.1145/3465481.3469205
      * Christos Grigoriadis, Spyridon Papastergiou, Panayiotis Kotzanikolaou, Christos Douligeris, Antreas Dionysiou, Elias Athanasopoulos, Karin Bernsmed, Per Håkon Meland and Liina Kamm. *Integrating and Validating Maritime Transport Security Services: Initial results from the CS4EU demonstrator*. Proceedings of the IC3 '21: 2021 Thirteenth International Conference on Contemporary Computing (IC3-2021), ACM DL, pp: 371-377, ACM, Noida (India), 2021. <https://doi.org/10.1145/3474124.3474213>
      * Panagiotis Bountakas, Konstantinos Koutroumpouchos, Christos Xenakis. *A Comparison of Natural Language Processing and Machine Learning Methods for Phishing Email Detection*. International Workshop on Advances on Privacy Preserving Technologies and Solutions (IWAPS 2021) held in conjunction with the 16th International Conference on Availability, Reliability and Security, ACMARES 2021 Conference, 2021. <https://doi.org/10.1145/3465481.3469205>
      * Maria Papathanasaki, Panagiotis Fountas, Leandros Maglaras, Christos Douligeris, Mohamed Amine Ferrag. *Quantum Cryptography in Maritime Telecommunications*. IEEE International Conference on Cyber Security and Resilience (CSR), pp: 530-535, 2021. 10.1109/CSR51186.2021.9527973
      * Vassilis Papaspirou, Leandros Maglaras, Mohamed Amine Ferrag, Ioanna Kantzavelou, Helge Janicke, Christos Douligeris. *A novel Two-Factor HoneyToken Authentication Mechanism,* 2021 International Conference on Computer Communications and Networks (ICCCN).

<https://doi.org/10.48550/arXiv.2012.08782>

* + - * Gencer Erdogan, Enrique Garcia-Ceja, Åsmund Hugo, Phu H. Nguyen, Sagar Sen. *A Systematic Mapping Study on Approaches for Al-Supported Security Risk Assessment.* 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC). IEEE Xplore, pp: 755 – 760, July 2021. <https://doi.org/10.1109/COMPSAC51774.2021.00107>
      * Said Daoudagh, Eda Marchetti, Vincenzo Savarino, Roberto Di Bernardo, Marco Alessi. How to Improve the GDPR Compliance through Consent Management and Access Control. Proceedings of the 7th International Conference on Information Systems Security and Privacy, ICISSP 2021,

pp: 534-541, SCITEPRESS. Online Conference, [2021.](https://www.scitepress.org/Papers/2021/102602/102602.pdf)

<https://www.scitepress.org/Papers/2021/102602/102602.pdf>

* + - * Antonello Calabrò, Said Daoudagh, Eda Marchetti. *MENTORS: Monitoring Environment for System of Systems.* Proceedings of the 17th International Conference on Web Information Systems and Technologies, WEBIST 2021, pp: 291—298, SCITEPRESS. Online Conference. <https://doi.org/10.5220/0010658900003058>
      * Said Daoudagh, Eda Marchetti. *GRADUATION: A GDPR-based Mutation Methodology*. Quality of Information and Communications Technology, QUATIC 2021. Communications in Computer and Information Science, vol 1439, pp: 311—324, Springer, Cham. Online Conference. <https://doi.org/10.1007/978-3-030-85347-1_23>
      * Bour, G., Bernsmed, K., Borgaonkar, R., Meland, P.H. *On the Certificate Revocation Problem in the Maritime Sector*. In: Asplund, M., Nadjm-Tehrani, S. (eds) Secure IT Systems. NordSec 2020. Lecture Notes in Computer Science, vol 12556, pp: 142-157. Springer, Cham, March 2021. <https://doi.org/10.1007/978-3-030-70852-8_9>
      * Jan Bobolz, Fabian Eidens, Stephan Krenn, Sebastian Ramacher, Kai Samelin. *Issuer-Hiding Attribute-Based Credentials.* 20th International Conference on Cryptology and Network Security (CANS 2021), Springer, LNSC,volume 13099 pp: 158-178, Vienna (Austria) [10.1007/978-3-030-](https://link.springer.com/chapter/10.1007/978-3-030-92548-2_9)

[92548-2\_9](https://link.springer.com/chapter/10.1007/978-3-030-92548-2_9)

* + - * Stephan Krenn and Thomas Lorünser. *Single-Use Delegatable Signatures from Smart Contracts.* International Conference on Availability, Reliability and Security (ARES 2021), ACM. Article 40, pp: 1-7. Vienna. <https://doi.org/10.1145/3465481.3469192>
      * Kasinathan, P., Martintoni, D., Hofmann, B., Senni, V., & Wimmer, M. *Secure Remote Maintenance via Workflow-Driven Security Framework.* 2021 IEEE International Conference on Blockchain (Blockchain), pp: 29-[37. 10.1109/Blockchain53845.2021.00016](https://ieeexplore.ieee.org/document/9680512)
      * João S. Resende, Marco Almeida, Rolando Martins, Luís Antunes. *A Kolmogorov Complexity for multidisciplinary domains.* Entropy 2021: The Scientific Tool of the 21st Century session Information Theory, Probability and Statistics, MDPI. <https://doi.org/10.3390/Entropy2021-09755>
      * Matthias Beckerle; Argyro Chatzopoulou; Simone Fischer-Hübner. *Towards Cybersecurity MOOC Certification.* In 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Vienna. 10.1109/EuroSPW54576.2021.00008
      * Antreas Dionysiou and Elias Athanasopoulos. *Unicode Evil: Evading NLP Systems Using Visual Similarities of Text Characters.* AISec '21: Proceedings of the 14th ACM Workshop on Artificial Intelligence and SecurityNovember 2021, pp: 1–12. <https://doi.org/10.1145/3474369.3486871>
      * Orpheas van Rooij, Marcos Antonios Charalambous, Demetris Kaizer, Michalis Papaevripides, and Elias Athanasopoulos. *webFuzz: Grey-Box Fuzzing for Web Applications.* In: Bertino, E., Shulman, H., Waidner, M. (eds) Computer Security – ESORICS 2021. ESORICS 2021. Lecture Notes in Computer Science, vol. 12972. Springer, Cham. <https://doi.org/10.1007/978-3-030-88418-5_8>
      * Antreas Dionysiou, Vassilis Vassiliades and Elias Athanasopoulos. *HoneyGen: Generating Honeywords Using Representation Learning.* ASIA CCS '21: Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security. 2021, pp: 265–279 <https://doi.org/10.1145/3433210.3453092>
      * Pachilakis, Michalis, Panagiotis Papadopoulos, Nikolaos Laoutaris, Evangelos P. Markatos, and Nicolas Kourtellis. *YourAdvalue: Measuring Advertising Price Dynamics without Bankrupting User Privacy*. Proceedings of the ACM on Measurement and Analysis of Computing Systems. Volume 5, Issue 3, 2021. Article No.: 32, pp 1–26. <https://doi.org/10.1145/3491044>
      * Emmanouil Papadogiannakis, Panagiotis Papadopoulos, Nicolas Kourtellis, Evangelos P. Markatos. User *Tracking in the Post-cookie Era: How Websites Bypass GDPR Consent to Track Users.* WWW '21: Proceedings of the Web Conference 2021. Pp: 2130–2141. <https://doi.org/10.1145/3442381.3450056>
      * Duc Ly Vu, Ivan Pashchenko, Fabio Massacci. *Please hold on: more time = more patches?*
      * *Automated program repair as anytime algorithms.* ICSE '21: Proceedings of the ACM/IEEE 43nd International Conference on Software Engineering Workshops. (APR), 2021, pp. 9-10, <https://ieeexplore.ieee.org/document/9474528>
      * Giorgio Di Tizio and Fabio Massacci. *A Calculus of Tracking: Theory and Practice.* Proceedings of the 25th International Conference of Financial Cryptography and Data Security, 2021. LNCS 12675, pp: 579-598 [10.1007/978-3-662-64331-0\_30](https://link.springer.com/chapter/10.1007/978-3-662-64331-0_30)
      * Duc Ly Vu, Fabio Massacci, Ivan Pashchenko, Henrik Plate, and Antonino Sabetta. *LastPyMile: identifying the discrepancy between sources and packages. ESEC/FSE'21:* Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering, 2021, pp: 780–792. [https://doi.org/10.1145/3468264.3468592](https://dl.acm.org/doi/abs/10.1145/3468264.3468592)
      * Gamal Elkoumy; Alisa Pankova; Marlon Dumas. *Mine Me but Don’t Single Me Out: Differentially Private Event Logs for Process Mining.* Proceedings of 3rd International Conference on Process Mining ICPM), 2021, pp. 80-87[, doi: 10.1109/ICPM53251.2021.9576852.](https://ieeexplore.ieee.org/document/9576852)
      * Mark F. St. John; Grit Denker; Peeter Laud; Karsten Martiny; Alisa Pankova; Dusko Pavlovic. *Decision Support for Sharing Data using Differential Privacy.* Proceedings of IEEE Symposium on Visualization for Cyber Security (VizSec) 2021, pp. 26-35, [doi: 10.1109/VizSec53666.2021.00008](https://ieeexplore.ieee.org/document/9629406).
      * Grigoriadis, Christos; Papastergiou, Spyridon; Kotzanikolaou, Panayiotis; Douligeris, Christos; Dionysiou, Antreas; Athanasopoulos, Elias; Bernsmed, Karin; Meland, Per Hakon; Kamm, Liina. *Integrating and Validating Maritime Transport Security Services: Initial results from the CS4EU demonstrator.* Proceedings of IC3 '21: 2021 Thirteenth International Conference on Contemporary Computing (IC3-2021), pp: 371–377, ACM. [https://doi.org/10.1145/3474124.3474213](https://dl.acm.org/doi/10.1145/3474124.3474213)
      * Chaudhary, S.; Kompara, M.; Pape, S. and Gkioulos, V, *Properties for Cybersecurity Awareness Posters' Design and Quality Assessment*, ARES 2022: The 17th International Conference on Availability, Reliability and Security, Vienna, 23 - 26 August 2022, ETACS 2022 https://dl.acm.org/doi/10.1145/3538969.3543794
      * Harborth, D. and Pape, S., *A Privacy Calculus Model for Contact Tracing Apps: Analyzing the German Corona-Warn-App*., ICT Systems Security and Privacy Protection - 37th IFIP TC 11 International Conference, SEC 2022, pages 3-19, IFIP Advances in Information and Communication Technology 648, 2022. http://dx.doi.org/10.1007/978-3-031-06975-8\_1
      * Bracamonte, V.; Pape, S. and Löbner, S., *"All apps do this": Comparing Privacy Concerns Towards Privacy Tools and Non-Privacy Tools for Social Media Content*, Proceedings on Privacy Enhancing Technologies (PoPETs), 2022 (3): 57-78, 2022, http://dx.doi.org/10.2478/popets-2022-0062
      * Pape, S.; Harborth, D. and Kröger, J. L, *Privacy Concerns Go Hand in Hand with Lack of Knowledge: The Case of the German Corona-Warn-App*, in ICT Systems Security and Privacy Protection - 36th IFIP TC 11 International Conference, SEC 2021, pages 256-269, Springer, IFIP Advances in Information and Communication Technology 625, http://dx.doi.org/10.1007/978-3-030-78120-0\_17
      * Pape, S., *Challenges for Designing Serious Games on Security and Privacy Awareness*, in Privacy and Identity Management. Between Data Protection and Security - 16th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Privacy and Identity 2021, Virtual Event, August 16-20, 2021, Revised Selected Papers, pages 3-16, Springer, IFIP Advances in Information and Communication Technology 644, http://dx.doi.org/10.1007/978-3-030-99100-5\_1

### Book Chapters

* + - * Shukun Tokas, Gencer Erdogan. *A need for privacy assistive technology in notice and consent paradigm.* Springer series Communications in Computer and Information Science (CCIS), to appear in January 2023.
      * Kettemann, M.; Peukert, A.; Spiecker gen. Döhmann, I. (Ed.). The Law of Global Digitality. Legal, Ethical & Social Aspects of IT, Taylor & Francis Group, London 2022.
      * Spiecker gen. Döhmann, I. § 71: *Grundrechte der Digitalisierung*. Kahl/Ludwigs (Ed.), Handbuch des Verwaltungsrechts, Bd. III, pp. 535-564. 978-3-955-99069-5. C.F. Müller, Köln, 2022.
      * Spiecker gen. Döhmann, I. *The More the Merrier*. In *The Law of Global Digitality,* pp- 77-95. Taylor & Francis Group, London 2022.
      * Silvia Vidor. COVID e sovranità tecnologica. *Il ruolo delle applicazioni per il tracciamento dei contatti.* CASD, 2022, pp: 505-511, Italy.
      * Hans Graux. *The Single Digital Gateway Regulation as an Enabler and Constraint of Once-Only in Europe.* The Once-Only Principle. Lecture Notes in Computer Science, pp. 83-103, Springer. Cham 2021.
      * Jesús Garcıa-Rodríguez, David Goodman, and Stephan Krenn. *From Research to Privacy- Preserving Industry Applications.* IFIP Summer School on Privacy and Identity Management 2022, Springer, December 2022 / January 2023
      * Sipola, T., Kokkonen, T., Karjalainen M., *Model Fooling Threats Against Medical Imaging*, Artificial Intelligence and Cybersecurity. Theory and Applications. Ed. by Tuomo Sipola, Tero Kokkonen, and Mika Karjalainen, pp 291-301, 2022, ISBN: 978-3-031-15030-2, 10.1007/978-3-031-15030-2\_13
      * Sipola, T., Puuska, S. & Kokkonen, T., *Model Fooling Attacks Against Medical Imaging: A Short Survey,* Information & Security: An International Journal 46, no. 2, pp 215-224, 2020, ISSN: 1314-2119, 10.11610/isij.4615
      * Kokkonen T. , Sipola T., Päijänen J., Piispanen J., *Cyber Range Technical Federation: Case Flagship 1 Exercise*, Collaborative Approaches for Cyber Security in Cyber-Physical Systems in Advanced Sciences and Technologies for Security Applications  
        Contact points, 2022, ISBN: 978-3-031-16087-5

### Books

* + - * *Stories – The narrative of a European cybersecurity community*, published by CyberSec4Europe, Brussels, November 2022
      * *Blue Book - A set of cybersecurity roadmaps and challenges for researchers and policymakers*, published by CyberSec4Europe, Heraklion, December 2022
      * David Goodman, Justine Phillips, Matt Stamper*, Data Privacy Program Guide, How to Build a Privacy Program that Inspires Trust,* CISO DRG Publishing, ISBN 978-1955976-11-4, 2022

### PhD Thesis or MSc Thesis

* + - * Per Håkon Meland. *Storyless cyber security: Modelling threats with economic incentives.* PhD Thesis, 2021. <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2825312>
      * Said Daoudagh. *The GDPR Compliance Through Access Control Systems*. PhD Thesis. University of Pisa, 2021. <https://etd.adm.unipi.it/theses/available/etd-07112021-124810/>
      * Jayavarshini Thirumalai. *An integrated approach for certification and re-certification based on the case study of an integrated circuit.* University of Turtu, 2021.

### Summer Schools

Here, we list the summer schools at which CyberSec4Europe partners participated. Details can be found in [D9.24].

* + - * IFIP Summer School on Privacy and Identity Management; Steering Committee: GUF, KAU, AIT besides several members in the Progam Committee. August 2022.
      * Hands-on tutorial for selected open-source tools from CS4E (seccerts,SCRUTINY, booltest) for EDUC summer school students (two sessions), Cagliari, June 2022.

### Organisation of Events (Conference and Workshops)

The consortium of CyberSec4Europe organized two main events, CONVERGENCE NEXT, held in June 2022 and MOMENTUM held in December 2022 both in Brussels and via live streaming. The first one was held in conjunction with the other pilots as its main objective was to show the demonstrators and the focus groups. The second one was intended to present to the community the main results of CyberSec4Europe.

Besides these events the members of the CyberSec4Europe consortium were involved in the organisation of other events. They are listed below:

GUF

* + - * 11. IT-Rechtstag Frankfurt. Held in Frankfurt, November 2022.
      * Workshop ´Jahrestagung Gesellschaft für Informatik: Recht und Technik im Diskurs`, September 2022 in Hamburg.
      * 10. IT-Rechtstag Frankfurt, online, November 2021.
      * Annual Privacy Forum 2021, online, June 2021.
      * Research Workshop: Cybersecurity and Machine Learning, online, May 2021. BRNO
      * Hands-on tutorials and cybersecurity games for training of the Czech national team participating in the European Cyber Security Challenge. July, August 2022, Brno.

CYBER

* + - * Insights webinar 'Introducing Fixed-Time Cybersecurity Evaluation Methodology for ICT Products (FITCEM/prEN 17640)', July 2021. online.

TDL

* + - * 'Privacy preserving industry applications from research to innovation'. Workshop organized together with AIT in conjunction with the 17th IFIP Summer School on Privacy and Identity Management. September 2022. Online.
      * 'Benefits and risks of emerging technologies and the GDPR'. Evening panel discussion moderated by TDL. February 2022, online. [https://cybersec4europe.eu/events/cybersec4europe-evening- panel-discussions/benefits-and-risks-of-emerging-technologies-and-the-gdprxx/](https://cybersec4europe.eu/events/cybersec4europe-evening-panel-discussions/benefits-and-risks-of-emerging-technologies-and-the-gdprxx/)
      * 'Community perspectives on the future of cybersecurity in Europe'. Evening panel discussion online, November 2021.
      * 'Cross-border data flows'. Evening panel discussion, online, July 2021.
      * Insight webinar 'Cybersecurity & Standards – How StandICT.eu supports European specialists in the international landscape', online, July 2021.
      * 'SME cybersecurity resilience in Europe'. Evening panel discussion, online, May 2021.
      * Insight webinar, 'Developments in European regulations', online, May 2021.
      * 'Establishing the Competence Centre in Bucharest and building the network'. Evening panel discussion, online, February 2021.
      * Insights webinar 'Towards more transparent security certifications – mining Common Criteria and FIPS140-2 certificates', online, February 2021.

TUD

* + - * Workshop within the 17th IFIP Privacy and Identity Management summer school for presenting the results of three of the pilots (specifically smart city of Murcia in UMU's case), September 2022, online.
      * Workshop “Building sustainable cybersecurity community: CyberSec4Europe lessons learned”. Together with the IFIP EGOV-CeDEM-ePart. September 2021, Granada.

UMU

* + - * Workshop at the 16th IFIP Privacy and Identity Management summer school where the ideas behind the technologies (p-ABCs, distributed oblivious authentication...) and their application to improve the CyberSec4Europe use case were recounted, August 2021, online.

ABI

* + - * Several meetings of the Cyber Knowledge and Security Awerness WG of CERTFin, during which the Constituency was updated on the progress of all European projects. February, May, July and September 2022.

AIT

* + - * International Conference on Cryptology and Network Security (CANS 2021). General Chair: AIT, December 2022. Vienna.

TLEX

* + - * Role playing session on reporting a (personal) data breach aimed to make participants aware of cyber security risks that may lead to data breaches, how to react to data breaches and how to prevent data breaches in the future, at the Summer Academy for Global Privacy Law 2022, Engineering data regulation(s) in an age of reform, June 2022, Brussels.

UM

* + - * Event on current state of cybersecurity in Slovenia and the future of cybersecurity in Slovenia and EU, including presentations from the four pilot projects and a round table involving the four projects and the (at the time acting) director of what will become the National Coordination Centre. October 2021, Ljubljana.

UMA

* + - * 16th International Conference on Network and System Security, Denarau Island, Fiji, 9-12 December 2022.
      * 3rd Joint Workshop on CPS & IoT Security and Privacy (CPSIoTSec 2022), Los Angeles, 7 November 2022.
      * 24th International Conference, ICICS 2022, Canterbury, 5-8 September 2022 4th International workshop in Artificial Intelligence and Industrial Internet-of-Things Security (AIoTS), Rome, 20-23 June 2022.
      * VI Jornadas Nacionales de Investigación en Ciberseguridad (JNIC2021 LIVE), online 9- 10 June 2021.
      * 2nd Joint Workshop on CPS & IoT Security and Privacy (CPSIoTSec 2021), online, 15 November 2021.

### Presentations at Events

Cyber Sec4Europe partners presented the proiect at the following events:

GUF

* + - * Invited talk on "Boundaries of Data Protection and IT-Security". October 2022, Sapienza university, Rome (Italy).
      * Panel " EU Cybersecurity Competence Centre" at IFIP Sec 2021, held online in June 2021.
      * Cybersec4Europe at SENSYBLE Workshop/Seminar, organized by SENSYBLE Graduate School by GUF and Rhein-Main University of Applied Sciences Wiesbaden, June 2021. Online event.
      * Panel presentation "Building the Cybersecurity Competence Center " at the Cybershare Conference 2021, May 2021.
      * CyberSec4Europe Aiming to safeguard values through excellence in cybersecurity" at Panel "The EU Pilot Projects for the competence centre and ECSO", at ITASEC 2021 conference, online April 2021.
      * "CyberSec4Europe Aiming to safeguard values through excellence in cybersecurity" at Panel "The EU Pilot Projects for the competence centre and ECSO", April 2021, online.
      * Panel presentation on AI for resilience and collaborative mitigation strategies for AI-driven response to cyber threats, Online March 2021 at LAILEC 2021, organized by KUL.
      * Cybersecurity Standardization Conference 2020, event organized by ENISA in February 2021 online.
      * A workshop on Security, Datenschutz und Anonymisierung, at Informatik 2021, Datenschutz und -sicherheit im Internet der Dinge, 28 September 2021, online
      * A presentation on "Serious Games for Security and Privacy Awareness" at the IFIP Summer School on Privacy and Identity Management, August 2021, online
      * A presentation on 'Human Factors in Security Management, Social Engineering & Privacy Enhancing Technologies' at the SECUSO Research Seminar, March 2021, online
      * A presentation on 'Privacy Concerns Go Hand in Hand with Lack of Knowledge: The Case of the German Corona-Warn-App' at SEC 2021, June 2021, online
      * A presentation on "A Privacy Calculus Model for Contact Tracing Apps: Analyzing the German Corona-Warn-App" at SEC 2022, June 2022, online

BRNO

* + - * Presentation of JCAlgTest on SECRYPT security conference. July 2022, Lisbon.
      * Webinar organized by CyberSec4Europe on open tool for analysis of security certificates issued under Common Criteria and FIPS schemes, February 2021.

CYBER

* + - * Panel about “Advances in Security Standards” at the IEEE Conference on Standards for

Communications and Networking (IEEE CSCN). November 2022, Thessaloniki.

* + - * Privacy-preserving-precision-medicine, KRAKEN project webinar Women in technology behind data-sharing, privacy preservation and SSI, May 2022. Online.
      * Bootcamp for EU cybersecurity team candidates, March 2022, The Hague. TDL
      * Added value of data exchanges, data marketplaces and the role of data intermediaries. ENISA Workshop on Data Sharing & Emerging Technologies, October 2022, in Brussels and online.
      * 'Europe’s Cybersecurity Community: The ECCC, the NCCs and the wider community' presented in the pitch area at the EU Pavilion at FIC 2022, Lille, 9 June 2022.
      * 'Cybersecurity for SMEs' presented during the GEIGER project session in the pitch area at the EU Pavilion at FIC 2022, Lille, 8 June 2022.
      * Panel on Smart Consent Management at the 2022 Privacy Symposium Conference (together with UMU). Held in Venice in April 2022.
      * Panel on CyberSec4Europe - Research to Innovation: Common Research Framework on Security and Privacy. at the 2022 Privacy Symposium Conference (moderated together with UMU). Held in Venice in April 2022. UNITN, POLITO, CNRS-IRIT, NTNU, ENG, CNR, ATOS, KUL and SINTED presented their work on the project.
      * Cybersecurity insights: emerging threats in Europe. Event organized by the project SOTER. Online, December 2021.
      * Cybersecurity solutions for the European finance sector. Event organized by the project SOTER. Online, October 2021.
      * 'Reasonable Security' within the IoT week, Global Vision: IOT today and beyond conference. In Dublin and online, June 2022.
      * Best practices and new developments in CyberSec4Europe at the 12th International Conference Days of Corporate Security 2021, organized by the ICS Institute, Slovenia and held online in May 2021.

TUD

* + - * LDE AI Mixer on disinformation and fake news: Disarming disinformation with AI. Leiden, September 2022.
      * Pre-conference interactive talk show during the ONE Conference, organized by Dcypher, September 2021. The Hague.

UNITN

* + - * Panel discussion in webinar "Professionalism in cybersecurity - current practice & outlook", IT Professionalism Europe (UNITN), Online November 2021.
      * Workshop ETACS (III): panel discussion "on current issues and trends in cybersecurity training and education", August 2021, Sparta.

AIT

* + - * Participation to Privacy Symposium for presenting T5.3, April 2022, Venice. ATOS
      * Presentation of the outcomes of Medical Data Exchange demonstrator during the webinar organized

by the OPEN DEI project, held online in September 2022.

* + - * Presentation of outcomes of Medical Data Exchange demonstrator to Centre de Seguretat de la Informació de Catalunya (CESICAT), June 2022.

ENG

* + - * During the MIM4 Workshop session in MyData in the Netherlands, the smart city use case of Municipality of Genova has been presented as well as how CyberSec4Europe is contributing on the collection of challenges, solutions and recommendations in the smart cities area to foster business models based on personal data exchange and usage in Smart City and Public Services. Amsterdam, November 2021.

ISGS

* + - * Incident Reporting Harmonization - workshop with EBA on the project regarding the reporting of ICT related incident, virtual, September 2021.
      * Workshop aimed at discussing cyber incident reporting advantages and the benefits of Cyber Lexicon, July 2021, online.

JAMK

* + - * Ihanus, J., Kokkonen, T., & Hämäläinen, T., *Modelling Medical Devices with Honeypots : A Conceptual Framework*, Information Systems and Technologies. WorldCIST 2022, Lecture Notes in Networks and Systems, vol 468, pp 144-155, 2022, ISBN: 978-3-031-04826-5, 10.1007/978-3-031-04826-5\_15
      * Alatalo, J., Sipola, T., Kokkonen, T., *Detecting One-Pixel Attacks Using Variational Autoencoders*, Information Systems and Technologies. WorldCIST 2022, Lecture Notes in Networks and Systems, vol 468., pp 611-623, 2022, ISBN: 978-3-031-04825-8, 10.1007/978-3-031-04826-5\_60
      * Karinsalo, A., Saharinen, K., Päijänen, J., Salonen, J., *Pedagogical and self-reflecting approach to improving the learning within a cyber exercise*, Proceedings of the 21st European Conference on Cyber Warfare and Security, ECCWS 2022. Vol. 21, No. 1, pp 105-114, 2022, ISBN: 978-1-914587-41-2, 10.34190/eccws.21.1.221
      * Päijänen, J., Saharinen, K., Salonen, J., Sipola, T., Vykopal, J. & Kokkonen, T., *Cyber range: preparing for crisis or something just for technical people?,* in Thaddeus Eze, Lee Speakman, Cyril Onwubiko (Eds.) Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021, pp 322-330, 2021, ISBN: 978-1-912764-43-3, 10.34190/EWS.21.012
      * Kokkonen T. , Päijänen J, Sipola T., *Multi-National Cyber Security Exercise, Case Flagship 2*, 14th International Conference on Education Technology and Computers (ICETC 2022), 2022, ISBN: 978-1-4503-9777-3, 10.1145/3572549.3572596
      * Janne Jaurimaa, Karo Saharinen and Sampo Kotikoski, Critical infrastructure protection -Employer expectations for cyber security education in Finland, In Thaddeus Eze, Lee Speakman, Cyril Onwubiko (Eds.) Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021, pp 195-202, 2021, ISBN: 978-1-912764-43-3, 10.34190/EWS.21.012

KAU

* + - * Panel on IT seccuity at the IFIPSec 2022 conference. Copenhagen, September 2022. SINTEF
      * Naval risks in the cyber domain. At the event Promoting a Free and Open Indo-Pacific: Naval

Incident Management in Asia and Europe organized by Stockholm International Peace Research Institute. Online, September 2022.

* + - * A Need for Privacy Assistive Technology in Notice and Consent Paradigm, June 2022 at the Privacy Symposium 2022, Venice
      * Privacy-(un)aware Internet of Things at the Public seminar on artificial intelligence and privacy, February 2022.

TLEX

* + - * Presentation on the topic 'Setting up of the European Cybersecurity Competence Network and Centre: where do we stand?'; explaining the role of CS4E. Organized by the Cyber and Data Security Lab, Vrje University of Brussels, November 2022.
      * New security obligations under the eIDAS 2 proposal; informal interventions referencing CS4E efforts and activities. eIDAS.2 - Enabling Interoperable Europe, organized by EEMA, Copenhagen, November 2022.
      * AI regulation; informal interventions referencing CS4E efforts and activities. At the Regulating Artificial Intelligence - Liability, personhood and procurement, June 2022. Organized by NOMIKI BIBLIOTHIKI SA PUBLISHING, EDUCATION & INNOVATION GROUP.
      * Discussion of the legal aspects of cryptocurrencies, including cybersecurity and criminal concerns. European Commission (DG Informatics’ IT Security Policy Unit), Webinar organized by the European Commission (DG Informatics’ IT Security Policy Unit) on Blockchain and cryptocurrencies: how to address their cybersecurity challenges?, May 2022, online.
      * Training on the conduction of GDPR audits and the preparation for such audits. On the Checking GDPR compliance: how do you conduct a data protection audit, & how do you prepare to be audited?, University of Tilburg, November 2021.

UM

* + - * Display/introduction of the Project on the 33rd Central European Conference on Information and Intelligent Systems’ website . Varaždin (Croatia), October 2021.

UMA

* + - * On the evolution of OCPP-based Charging Infrastructures: Threats and Countermeasures”, The Second International Symposium on Emerging Information Security and Applications (EISA), November 2021.
      * Panel “From Education through Smart Industry passing by R&D”, JNIC 2021 LIVE, 9-10 June 2021.

## Business

ATOS participated in the following events:

* + - Market Deployment, Investments and International Collaboration Members Meeting held by ECSO in The Hague in October 2022.
    - Presentation of the paper Governance Mesh Approach for Cybersecurity Ecosystem at Digilience conference organized by pilot project ECHO, September 2020, Plovdiv, Bulgaria.
    - Workshop Building a Robust Cyber Ecosystem – Lessons from the EU as speaker held in Sarajevo, June 2022.
    - Panel on Market Incentives for Certification, organized by ENISA in Athens and online in June 2022.
    - Global Reach - World Economic Forum Annual Meeting in Davos - “Strengthening trust in public- private data exchanges” Roundtable
    - Two presenters at a workshop organized by the Data Protection Office: CyberSec4Europe - Research to Innovation: Privacy-preserving Industry Application Innovations, Venice, April 2022.

GUF participated in the following events:

* + - EP ITRE public hearing on “European Digital Identity Wallet and Trust Services”. Brussels and online. February 2022.
    - ECSO board of directors, general assembly and WG1 meeting, held on 30th June-1st of July. Online.
    - Participation meetings DIN KITS (German Expert Advisory Group for Cybersecurity), June 2021, online.
    - Impulse speech "Data Protection in the context of IoT" at German-Japanese iSec Expert Meeting #46. June 2021, online.
    - Keynote Standards in Privacy Management: Assurance to demonstrate accountability at Privacy Symposium 2021, June 2021 online.
    - Europäische Cyber Security Strategie am Beispiel des Cyber Security Competence Center Networks CyberSec4Europe at ECSEL-Austria Konferenz. Industrial Cyber Security, held online April 2021.
    - Impulse Speech "CyberSec4Europe Aiming to safeguard values through excellence in cybersecurity" at Austria Industriellenvereinigung, Arbeitsgruppe 3 „Connectivity, Infrastructure and Cybersecurity“ Task Force „Digitalisierung und Künstliche Intelligenz, online Februry 2021.

BRNO

* + - Presentation of open tool for analysis of security certificates issued under Common Criteria and FIPS schemes, focus on usage by industry, online. March 2021.
    - Presentation of a lab environment created by Cyber Sandbox Creator to students of an introductory security course, online April 2021.

CYBER

* + - CyberSec4Europe Insights webinar on Developments in European Regulations. Webinar, May 2021.
    - ENISA/CEN-CENELEC/ETSI Cybersecurity Standardization Conference 2021: European Standardization in support of the EU Cybersecurity Act, February 2021, online.
    - CyberSec4Europe Insights series webinar on "Towards more transparent security certifications – mining Common Criteria and FIPS140-2 certificates", May 2021, online.
    - CyberSec4Europe Insights series webinar on Cybersecurity & Standards – How StandICT.eu supports European specialists in the international landscape, May 2021, online.

TDL

* + - Online meeting with ENISA concerning strategy for SMEs, September 2022.
    - Participated with other pilot projects on SME impact and opportunities at the conference organized by DIGITAL SME Alliance/ENISA focusing on SMEs held online in July 2021.

SIE

* + Presentation of T5.2 supply chain security demonstrator on the 2021 ECSEL conference on "Industrial Cyber Security". Presentation was done by GUF, Kai Rannenberg with support from SIE, online April 2021.

DAWEX

* + DAWEX participated in a panel on the Global Reach - World Economic Forum Annual Meeting in Davos - “Strengthening trust in public-private data exchanges” Roundtable, Davos, May 2022.

KAU

* + Invited talk and panel on usable privacy at the Nordic Data Privacy Forum, Stockholm, September 2022.

UMA

* + Cybersecurity Challenges in the digitalization of the Industry. Centro de Ciberseguridad Industrial, Madrid, April 2022.

## Governmental

* + - French Ministry of Economy - “The Role of Data Spaces” - Demonstration of Dawex technology with Agdatahub – France, September 2022.
    - SINTEF presented Privacy in Internet of Things for their government in April 2022.
    - SINTEF participated in the discussions on the progress of the NCCC. Several meetings held from June 2021 until December 2022 together with the Norwegian Research Council of the Ministry of Digitalization in Norway.
    - TDL and GUF organised a roundtable discussion on 'Community Perspectives On The Future of Cybersecurity in Europe'. Brussels, November 2021.
    - GUF maintained a discussion with Dr. Christoph Scholten (German Bundesministerium für Wirtschaft und Energie) as part of the Mercator Science-Policy Fellowship Program, June 2021, held online.
    - AIT participated in the “Personal Data Sharing - Emerging Technologies” workshop organized by ENISA in Brussels (Belgium) by presenting Research Activities on Data Sharing Use Cases. October 2022.

## Standardisation

The activities of standardization are more specified in more detail in WP8. However, we mentioned here the standardization bodies to which CyberSEc4Europe belong.

GUF participated in the following standardisation meetings:

* + - CEN/CLC JTC 13 for the Cybersecurity and Data Protection and WGs, July 2021
    - CEN/CLC CWA on Digital sovereignty, July 2021.
    - ISO/IEC JTC 001/SC 27/CAG "Chair’s Advisory Group", July 2021.
    - CEN/CLC JTC 13 Cybersecurity and Data Protection and WGs, July 2021, held online.
    - CEN/CLC JTC 13 Cybersecurity and Data Protection WG 5 "Data Protection, Privacy and Identity Management", online in June 2021.
    - ISO/IEC JTC 1/SC 27 WGs, especially WG 5 "Identity Management and Privacy Technologies", held online in June 2021.
    - DIN NIA 27 AA „IT-Sicherheitsverfahren“ (German Mirror Committee to SC 27) and DIN NIA 27 AKs (German Mirror Committees to SC 27 WGs). June 2021, held online.
    - Workshop "Analyse von Bedarfen der NRM KI zum Thema KI in der Medizin und IT-Sicherheit bei KI-Systemen", held online in May 2021.
    - ISO/PC 317 and ISO/PC 317/WG 1, online April 2021.
    - Consumer protection: privacy by design for consumer goods and services"
    - DIN NIA 27 AA „IT-Sicherheitsverfahren“ Delegation to SC 27, Online April 2021.
    - ISO/IEC JTC 1/SC 27 WGs, especially WG 5 "Identity Management and Privacy Technologies", held online in April 2021.
    - ISO/IEC JTC 001/SC 27/AG 03 "Concepts and Terminology", March 2021.
    - CEN/CLC JTC 13 Cybersecurity and Data Protection WG 1 "Chairman advisory group", online March 2021.
    - ISO/IEC JTC 001/SC 27/AG 06 "Operations", online March 2021.
    - ISO/IEC JTC 001/SC 27/AG 05 "Strategy", online March 2021.
    - CEN/CLC JTC 13 Cybersecurity and Data Protection WG 5 "Data Protection, Privacy and Identity Management", online March 2021.
    - Meetings CEN/CLC JTC 13 Cybersecurity and Data Protection and WGs, online March 2021.
    - Meeting CEPIS Legal and Security Issues (LSI) Network, online March 2021.
    - CEN/CLC JTC 13 Cybersecurity and Data Protection WG 5 "Data Protection, Privacy and Identity Management", online February 2021.
    - ISO/IEC JTC 001/SC 27/CAG "Chair’s Advisory Group", online February 2021.
    - ISO/IEC JTC 1/SC 27/WG 5 "Identity Management and Privacy Technologies", online February 2021.
    - DIN NIA 27 AK 05 (German Mirror Committee to ISO/PC 317), online February 2021.
    - CEN/CLC JTC 13 Cybersecurity and Data Protection WG 1 "Chairman advisory group", online February 2021.

AIT participated in the following standardisation events:

* + - Remote participation in (virtual) ASI AG 001.27 meeting (Austrian mirror committee of ISO/IEC JTC1/SC27), November 2022.
    - AIT members are working as editors in the following standardization documents:
      * ISO/IEC 23264-1 Information security — Redaction of authentic data — Part 1: General
      * ISO/IEC 23264-2 Information security — Redaction of authentic data — Part 2: Redactable signature schemes based on asymmetric mechanisms.
      * ISO/IEC 20009-3 Information technology — Security techniques — Anonymous entity authentication — Part 3: Mechanisms based on blind signatures concepts.
      * ISO/IEC 4922-1 Information security - Secure multiparty computation - Part 1: General.
      * ISO/IEC 4922-2 Information security — Secure multiparty computation — Part 2: Mechanisms based on secret sharing.
      * ISO/IEC 20008-2 Information technology — Security techniques — Anonymous digital signatures — Part 2: Mechanisms using a group public key.
    - 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.
    - Remote participation in (virtual) ASI AG 001.27 meeting (Austrian mirror committee of ISO/IEC JTC1/SC27), September 2022.
    - ZKProof. Sigma Protocols.

ATOS participated in the following standardisation events:

* + - Periodic ISO/IEC JTC1/SC27 (“Information security, cybersecurity and privacy protection”) working group meetings, held online in May 2022.

# 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](#_bookmark17) to which we have added the column of achievements up to the end of the project to the table that we showed in [D9.10]. 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activity** | **KPI/Target** | **Achieved**  M25-M47 | **Achieved M13-M24** | **Achieved M01-M12** |
| Flash studies, production of CyberSec4Europe leaflets | ≥ 3, one per annum |  | No new leaflets were produced due to the absence of in- person meetings | 9 |
| Participation in 6 public exhibitions and demonstrations | 3 per annum after M12 | 74 | 21 | Already achieved even though not expected until after M12 |
| Journal publications in international referred journals | More than 30 | 68 | 30 | 5 |
| Reviewed publications/ presentations in international conferences | More than 50 | 68 | 36 | 17 |
| CyberSec4Europe co- organised workshops | More than 2 workshops, each attended by more than 40 participants,with more than 20 | 27 | 9 | 7 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| CyberSec4Europe tutorials | More than 2 tutorials co-located with summer- schools, more than 1 in a relevant conference | 2 | 1 |  |
| Organization and hosting of 4 hackathons / pitstops | To take place after  M12 |  | 5 |  |
| 6 presentations at meetups | 2 per annum after M1 | 31 | 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 the end of the project

# Community Activities

DG CONNECT has worked closely with the four funded pilots (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. CyberSec4Europe has participated in several meetings either with all or some of the other three pilots and other agencies. These were the following:

* + TDL submitted a proposal on behalf of CyberSec4Europe to the European Commission consultations on the evolution of PSD2 (i.e., PSD3), in August 2022..
  + At FIC 2022 (the International Cybersecurity Forum) in Lille, June 2022, TDL moderated in the EU Pavilion pitch area on behalf of DG CONNECT featuring DG CONNECT, ENISA, Europol and other H2020 projects.
  + CyberSec4Europe and CONCORDIA organized the Workshop CYTILIS. Presentation on Threat intelligence in the financial sector by TDL, held online in December 2021.
  + International Cybersecurity Forum (FIC 2023) organized by DG CNECT, CONCORDIA, ECHO and SPARTA in Lille, September 2021. TDL represented CyberSec4Europe.
  + Synchronisation with the fellow pilot projects on research priorities harmonization, May 2021, online.
  + Synchronisation with DG CONNECT, REA and JRC and with the four pilot project coordinators and ECSO. May 2021.
  + ECSO WG6 Meeting on EC Roadmaps and Research Programs, April 2021 online.
  + Meeting of DG CONNECT, REA and JRC with the four pilot projects' coordinators and ECSO, held online and in Brussels in March 2021.
  + Synchronisation with DG CONNECT, REA and JRC and with the fellow pilot projects' coordinators and ECSO, held online and in Brussels in March 2021.
  + Financial sector federated learning. CyberSec4Europe/ CONCORDIA, March 2021. Online.
  + ECSO Board of Directors Meeting, March 2021 online.
  + GUF attended the meeting of the four pilot projects' Governance Coordination Group held online in February 2021.

Among these events and meetings, we can highlight CONVERGENCE and CONVERGENCE NEXT. Both were organised by CyberSec4Europe with the participation of the other three pilots and ECSO. These events were held in December 2021 (online) and June 2022 in Brussels and online.

Besides that, the four pilots together created focus groups in different areas. CyberSec4Europe attended the meetings of the following focus groups:

* + Communications Group (TDL):
    - Meeting held online in July 2022.
    - Meeting held online in May 2022.
    - Regular meeting in March 2022, online.
    - Social event, March 2022, also online.
    - Meeting held online in December 2021 (chaired by TDL).
    - Meeting held online in July 2021 (chaired by TDL).
    - Meeting held online in February 2021.
  + Threat Intelligence Focus Group (TDL, i-BP, UMU).
  + Cyber Range Focus Group (JAMK)
  + Roadmapping Focus Group (FORTH)
  + Education Focus Group (UNITN)
    - UNITN attended the meetings organized together with the pilots and ENISA on the WG on Education for the future CCN during 2021 and 2022.

# Summary

This deliverable is an update of [D9.10]. In this deliverable we have described the outreach activities carried out by CyberSec4Europe partners during the last two years of the project. We have described these activities by following the target audiences identified in ([D9.3]).

We have referenced the KPIs that measure 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, the outreach activities have been widely achieved.

In summary CyberSec4Europe have widely disseminated the results of their work to a large number of audiences including their intended target audiences, as witnessed by the around two hundred publications, almost one hundred conferences and around 50 events and wide participation in a multiplicity of forums across Europe.

# References

[D9.3] Dissemination and Awareness Plan

[D9.5] Report on the Outreach and Dissemination Activities 1 [D9.9] Deliverable D9.9: Website and Social Media Accounts 3 [D9.10] Report on the Outreach and Dissemination Activities 2 [D9.24] CyberSec4Europe summer school 3