HORIZON 2020

A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis

Resultados

Información del proyecto

CS-AWARE

Identificador del acuerdo de subvención: 740723

Sitio web del proyecto

DOI
10.3030/740723

Proyecto cerrado

Fecha de la firma de la CE
26 Abril 2017

Fecha de inicio
1 Septiembre 2017

Fecha de finalización
31 Agosto 2020

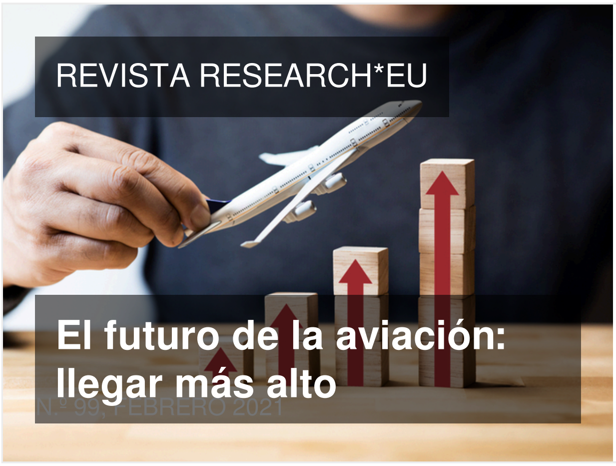
Financiado con arreglo a
Secure societies - Protecting freedom and security of Europe and its citizens

Coste total
€ 4 648 362,50

Aportación de la UE
€ 3 728 603,75

Coordinado por
OULUN YLIOPISTO
Finland

Este proyecto figura en...



CORDIS proporciona enlaces a los documentos públicos y las publicaciones de los proyectos de los programas marco HORIZONTE.

Los enlaces a los documentos y las publicaciones de los proyectos del Séptimo Programa Marco, así como los enlaces a algunos tipos de resultados específicos, como conjuntos de datos y «software», se obtienen dinámicamente de OpenAIRE.

Resultado final

Documents, reports (17)

CS-AWARE technical documentation and training material
This deliverable must be ready for the pilot, but may be enhanced during and after the pilots. Documentation will primarily be in electronic searchable form, and training material may comprise of different media types depending on the needs of the end-users. (written, video, computer animation and simulation exercises.)

Guidelines and procedures for system and dependency analysis in the context of local public administrations [
This deliverable contains the guidelines and procedures for system and dependency analysis in local public administrations that are defined in T2.4. This deliverable will be the basis for dissemination activities to relevant regulatory and standardisation bodies.

System and dependency analysis (third iteration) – Pilot scenario specification and self-healing strategies
This deliverable contains the final results of the system and dependency analysis based on the third iteration of general requirements analysis of T2.1 and pilot specific analysis of T2.2. This deliverable forms the final environment for tool

deployment and also contains the results for defining self-healing strategies within the pilot scenarios.

Design CS-AWARE common cloud-based software architecture and API specification

This includes visualisations of the overall final CS-AWARE architecture and list of APIs available with the necessary description and examples of usage.

Commercial actions report 3

This deliverable will document the latest developments regarding commercial actions taken.

Pilot evaluation report

This deliverable will contain a detailed report of the results obtained from the pilot case studies carried out within this project, including an evaluation of the practical relevance of and end user experiences with the cybersecurity mechanisms provided by the CS-AWARE solution (cybersecurity situational awareness, cybersecurity information sharing and self-healing).

System and dependency analysis (first iteration) – Cybersecurity requirements for local public administrations

This deliverable contains the first iteration of analysis results, with the purpose of defining the cybersecurity requirements for local public administrations. This deliverable is based on the first iterations of general requirements analysis of T2.1 and pilot specific analysis of T2.2. This deliverable is a direct input for T2.3.

CS-AWARE solution validation and testing report

Deliverable is based on T 4.4 and contains the validation and testing results of the CS-AWARE system before its final deployment.

Commercial actions report 2

This deliverable will document the latest developments regarding commercial actions taken.

Exploitation, dissemination and commercialisation report 3

This report will include all relevant information (both plan and performed activities) regarding the project exploitation, dissemination and commercialisation by the members of the consortium.

Pilot deployment report

This deliverable will contain a detailed report of the deployment of the CS-AWARE solution within the environments provided by the local public administrations that are part of this project.

Exploitation, dissemination and commercialisation report 2

This report will include all relevant information (both plan and performed activities) regarding the project exploitation, dissemination and commercialisation by the members of the consortium.

Commercial actions report 1

This deliverable will document the latest developments regarding commercial actions taken.

Exploitation, dissemination and commercialisation report

This report will include all relevant information (both plan and performed activities) regarding the project exploitation, dissemination and commercialisation by the members of the consortium.

System and dependency analysis (second iteration) – Pilot scenario definition

This deliverable refines the results of D2.1 based on the second iteration of analysis of T2.1 and T2.2. The analysis results is the basis for the pilot scenario definitions and provide input to the pilot deployment preparations.

CS-AWARE framework

This deliverable specifies the CS-AWARE framework defined in T2.3. Based on the initial analysis results presented in D2.1.1, this deliverable specifies the interrelation between the CS-AWARE building blocks as well as the relevant internal and external information sources to collect and share cybersecurity data. The CS-AWARE framework will be a requirement for the technical software architecture tasked in WP3.

User story report

This deliverable will contain a composition of user stories relating to the cybersecurity experiences of the CS-AWARE project in the context of local public administrations. This could be in the form of a report or a book, edited by the WP-leaders, entitled: Narratives on cybersecurity: implementation and lessons of the CS-AWARE project.

Other (1)

System and dependency analysis tool support adaptation

This deliverable includes the implemented and tested adaptation of the GraphingWiki tool to meet the needs of the CS-AWARE solution.

Websites, patent fillings, videos etc. (1)

[Project’s public website, leaflet and poster]
This deliverable essentially consists of the project’s website and any additional related material, such as leaflets, posters, etc. The website should be up by M3 and will be updated throughout the project duration.

Publicaciones

Book chapters (1)

[Challenges in Cybersecurity and Privacy - the European Research Landscape]
Autores: Thomas Schaberreiter Forschungsgruppe Multimedia Information Systems, Fakultät für Informatik, Universität Wien Juha Röning University of Oulu Gerald Quirchmayr Forschungsgruppe Multimedia Information Systems, Fakultät für Informatik, Universität Wien Veronika Kupfersberger Forschungsgruppe Multimedia Information Systems, Fakultät für Informatik, Universität Wien Chris Wills CARIS Resear
Publicado en: 2019, Página(s) 149-180
Editor: River Publishers Series in Security and Digital Forensics
DOI: 10.13052/rp-9788770220873

Conference proceedings (7)

An Information Flow Model to Support NIS Mandated Reporting
Autores: Quirchmayr, Gerald Kupfersberger, Veronika Langner, Gregor Schaberreiter, Thomas
Publicado en: 12th Conference on Autonomous Systems, Edición 23-30 Oct 2019, 2019, Página(s) 137-143, ISBN 978-3-18-386410-2
Editor: online

Exploring Knowledge Graphs in an Interpretable Composite Approach for Text Entailment
Autores: Vivian S. Silva, André Freitas, Siegfried Handschuh
Publicado en: Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-19). Honolulu, USA. 2019, Edición Annual, 2019
Editor: AAAI Press

[Security-Driven Information Flow Modelling for Component Integration in Complex Environments]
Autores: Veronika Kupfersberger, Thomas Schaberreiter, Gerald Quirchmayr
Publicado en: Proceedings of the 10th International Conference on Advances in

Information Technology - IAIT 2018, 2018, Página(s) 1-8, ISBN 9781-450365680
Editor: ACM Press
DOI: 10.1145/3291280.3291797

Addressing Complex Problem Situations in Critical Infrastructures using Soft Systems Analysis: The CS-AWARE Approach
Autores: Thomas Schaberreiter, Chris Wills, Gerald Quirchmayr and Juha Röning
Publicado en: SECURWARE 2017 : The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Edición Annual, 2017, Página(s) 99-105, ISBN 978-1-61208-582-1
Editor: IARIA XPS Press

Enhancing credibility of digital evidence through provenance-based incident response handling
Autores: Ludwig Englbrecht, Gregor Langner, Günther Pernul, Gerald Quirchmayr
Publicado en: Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19, 2019, Página(s) 1-6, ISBN 9781450371643
Editor: ACM Press
DOI: 10.1145/3339252.3339275

A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources
Autores: Thomas Schaberreiter, Veronika Kupfersberger, Konstantinos Rantos, Arnolnt Spyros, Alexandros Papanikolaou, Christos Ilioudis, Gerald Quirchmayr
Publicado en: Proceedings of the 14th International Conference on Availability, Reliability and Security - ARES '19, 2019, Página(s) 1-10, ISBN 9781450371643
Editor: ACM Press
DOI: 10.1145/3339252.3342112

An Innovative Self-Healing Approach with STIX Data Utilisation
Autores: Arnolnt Spyros, Konstantinos Rantos, Alexandros Papanikolaou, Christos Ilioudis
Publicado en: Proceedings of the 17th International Joint Conference on e-Business and Telecommunications, 2020, Página(s) 645-651, ISBN 978-989-758-446-6
Editor: SCITEPRESS - Science and Technology Publications
DOI: 10.5220/0009893306450651

Peer reviewed articles (2)

Interoperability Challenges in the Cybersecurity Information Sharing Ecosystem

Autores: Konstantinos Rantos, Arnolnt Spyros, Alexandros Papanikolaou, Antonios Kritsas, Christos Ilioudis, Vasilios Katos
Publicado en: Computers, Edición 9/1, 2020, Página(s) 18, ISSN 2073-431X
Editor: Computers
DOI: 10.3390/computers9010018

Applying Soft Systems Methodology to Complex Problem Situations in Critical Infrastructures: The CS-AWARE Case Study
Autores: Veronika Kupfersberger, Thomas Schaberreiter, Chris Wills, Gerald Quirchmayr and Juha Röning
Publicado en: International Journal On Advances in Security, Edición vol 11, no 3&4, year 2018, 2018, Página(s) 191 - 200, ISSN 1942-2636
Editor: IARIA Xpert Publishing Services

Otros productos de investigación

Otros productos de investigación a través de OpenAire (1)

Cybersecurity:you cannot neglect protecting essential services
Autores: Röning, J. (Juha)

Última actualización: 18 Agosto 2022

Permalink: https://cordis.europa.eu/project/id/740723/results/es