Secure Information Sharing Sensor Delivery event Network

Résultats

Informations projet

SISSDEN

N° de convention de subvention: 700176

Site Web du projet

DOI
10.3030/700176

Projet clôturé

Date de signature de la CE
21 Avril 2016

Date de début
1 Mai 2016

Date de fin
30 Avril 2019

Financé au titre de
Secure societies - Protecting freedom and security of Europe and its citizens

Coût total
€ 6 341 775,00

Contribution de l'UE
€ 4 912 692,50

Coordonné par
NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY
Pologne

CORDIS fournit des liens vers les livrables publics et les publications des projets HORIZON.

Les liens vers les livrables et les publications des projets du 7e PC, ainsi que les liens vers certains types de résultats spécifiques tels que les jeux de données et les logiciels, sont récupérés dynamiquement sur OpenAIRE.

Livrables

Documents, rapports (10)

Final legal requirements

Updated version of D2.2.

Final data analysis results

Final results of T5.1, T5.2 and T5.3, using T5.4 as the basis. The report will detail the advances made in this WP, including the novel insights derived from the individual and combined data sets and suggestions for fellow researchers.

Final dissemination report

Final version of D2.1, including data from the second reporting period.

Preliminary legal requirements

This deliverable will document the management of all legal aspects and deployment strategy, as well as the IPR management. Particular attention will be paid to the law differences among the member states as well as other Countries where SISSDEN will be operated, focusing on European level, but with paying attention to sensible regions outside Europe.

Qualitative and quantitative assessment report

Essential assessment of both the qualitative and quantitative success and impact of the SISSDEN pilot.

Data exchange interfaces specification

Specification of data exchange interfaces and mechanisms used in SISSDEN.

Trial definition and test plan

Technical trial and testing plan documents, updated regularly during the WP6 pilot phase to ensure successful testing of all SISSDEN pilot phase elements.

Metrics specification and results

This deliverable presents the final set of metrics derived from the data available to the consortium and their application for cross-country and cross-region comparisons. With interactive and searchable online metrics & statistical mapping.

Preliminary data analysis specification

The deliverable documents the new analyses developed in T5.1, T5.2 and T5.3, including a preliminary specification of new information they provide.

Interim dissemination report

This report is an instrument that will allow following the awareness actions done by the project partners throughout the project. The preliminary version will report past activities and give an overview of actions the planned in the second period,

while the final report will contain the list of all activities done at several dissemination level, such as papers, website, links from other reference websites, demonstrations and workshops.

Sites Web, dépôts de brevet, vidéos, etc. (3)

Collaboration and data sharing portals

This deliverable will consist of web services to support the collaboration and sharing of data inside the project and with external participants. The project website is public in general, but may contain non-public sections internal to the consortium.

Project website

The project website will be created at a very early stage of the project and will be kept updated all along project duration. This deliverable represents an important part of Task 2.4 and will be carried out by partners paying attention to exploit the website as a key dissemination and market approach instrument.

Platform user feedback system

Feedback platform to allow SISSDEN consortium members and other vetted system users to provide feedback on SISSDEN system usage.

Publications

Articles approuvés par les pairs (1)

Botnet Fingerprinting: Anomaly Detection in SMTP Conversations

Auteurs: Piotr Bazydlo, Krzysztof Lasota, Adam Kozakiewicz
Publié dans: IEEE Security & Privacy, Numéro 15/6, 2017, Page(s) 25-32, ISSN 1540-7993
Éditeur: IEEE Computer Society
DOI: 10.1109/MSP.2017.4251116

Actes de conférence (8)

Linking Amplification DDoS Attacks to Booter Services

Auteurs: Johannes Krupp, Mohammad Karami, Christian Rossow, Damon McCoy, Michael Backes
Publié dans: Research in Attacks, Intrusions, and Defenses. RAID 2017. Lecture Notes in Computer Science., 2016, Page(s) 427-449, ISBN 978-3-319-66332-6
Éditeur: Springer International Publishing
DOI: 10.1007/978-3-319-66332-6_19

Evasive Malware via Identifier Implanting
Auteurs: Rui Tanabe, Wataru Ueno, Kou Ishii, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Daisuke Inoue, Christian Rossow
Publié dans: Detection of Intrusions and Malware, and Vulnerability Assessment, Numéro 10885, 2018, Page(s) 162-184, ISBN 978-3-319-93410-5
Éditeur: Springer International Publishing
DOI: 10.1007/978-3-319-93411-2_8

teEther: Gnawing at Ethereum to Automatically Exploit Smart Contracts
Auteurs: Johannes Krupp, Christian Rossow
Publié dans: 27th USENIX Security Symposium (USENIX Security 18), Numéro August 15–17, 2018, 2018, Page(s) 1317-1333, ISBN 978-1-939133-04-5
Éditeur: USENIX Association

Millions of targets under attack - a macroscopic characterization of the DoS ecosystem
Auteurs: Mattijs Jonker, Alistair King, Johannes Krupp, Christian Rossow, Anna Sperotto, Alberto Dainotti
Publié dans: Proceedings of the 2017 Internet Measurement Conference on - IMC '17, 2017, Page(s) 100-113, ISBN 9781-450351188
Éditeur: ACM Press
DOI: 10.1145/3131365.3131383

MemScrimper: Time- and Space-Efficient Storage of Malware Sandbox Memory Dumps
Auteurs: Michael Brengel, Christian Rossow
Publié dans: Detection of Intrusions and Malware, and Vulnerability Assessment, Numéro 10885, 2018, Page(s) 24-45, ISBN 978-3-319-93410-5
Éditeur: Springer International Publishing
DOI: 10.1007/978-3-319-93411-2_2

MALPITY: Automatic Identification and Exploitation of Tarpit Vulnerabilities in Malware.
Auteurs: Sebastian Walla, Christian Rossow
Publié dans: 4th IEEE European Symposium on Security and Privacy, Numéro 4, 2019, Page(s) TBD (in print)
Éditeur: IEEE

Don't Trust The Locals: Investigating the Prevalence of Persistent Client-Side Cross-Site Scripting in the Wild

Auteurs: Marius Steffens, Christian Rossow, Martin Johns, Ben Stock
Publié dans: Proceedings 2019 Network and Distributed System Security Symposium, 2019, ISBN 1-891562-55-X
Éditeur: Internet Society
DOI: 10.14722/ndss.2019.23009

Świadomość sytuacyjna cyberzagrożeń (eng. Cyber-threat Situational Awareness)
Auteurs: Adam Kozakiewicz
Publié dans: Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne, Numéro 8-9, 2018, Page(s) 562-568, ISSN 1230-3496
Éditeur: Sigma-NOT

Autres (1)

Recurrent Neural Networks for Enhancement of Signature-based Network Intrusion Detection Systems
Auteurs: Sohi, Soroush M.; Ganji, Fatemeh; Seifert, Jean-Pierre
Publié dans: Numéro 1, 2018
Éditeur: arXiv.org

Chapitres d'ouvrage (1)

Cyber-Threat Intelligence from European-wide Sensor Network in SISSDEN
Auteurs: Edgardo Montes de Oca, Jart Armin, Angelo Consoli
Publié dans: Challenges in Cybersecurity and Privacy - the European Research Landscape, 2019, Page(s) 117-128, ISBN 9788-770220880
Éditeur: River Publishers

Dernière mise à jour: 20 Juillet 2023

Permalink: https://cordis.europa.eu/project/id/700176/results/fr