# **S CYBERSANE**

Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures

# Contents

EDITOR'S NOTE2
News & Events3
Press & Other Content4
Scientific Publications5
Meet the Partner6





This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833683



# **EDITOR'S NOTE**

During the last period started the WP9 where CyberSANE partners are going to define and perform the three project pilots: energy, transport, and health.

In the lasts months we have been working in the detailed description of the pilot scenarios including actors and systems involved, CyberSANE components to be used, conditions, and the execution flow.

Furthermore, partners have started to analyse and prepare the infrastructure needed for each of the pilots. In order to execute them, we need to acquire and install hardware, software, and devices.

**CYBER**SANE

In the next six months, once the CyberSANE components are developed and integrated, we will deploy them and plan the pilot events. We will also start preparing the training material for the end users and stakeholders. In addition, we will publish the D9.1 Report on Pilot Sites Preparation and Detailed Pilot Operations Planning, with all the preparation plans.

linkedin.com/company/cybersane-h220/
twitter.com/CyberSANEH2020
youtube.com/channel/UCPq40hl019Ha8cEqZVVmbaQ
www.cybersane-project.eu

# **News & Events**

FIND HERE THE MAIN HIGHLIGHTS OF CYBERSANE DISSEMINATION AND COMMUNICATION ACTIVITIES

Joint Standardisation Workshop Dynamic countering of cyber-attacks projects

## Joint Standardisation Workshop of Dynamic Countering of Cyber-Attacks Projects

**C Y B E R** S A N E

Jan 22, 2021

CyberSANE hosted the first Joint Standardisation Workshop along with projects from the SU-ICT-01-2018 H2020 call, whose main topic is Dynamic countering of cyber-attacks: C4IIoT, CARAMEL, GUARD, SAPPAN, SIMARGL, and SOCCRATES.





## CS4CA's 24H4 Global Cyber Security Summit

#### May 6, 2021

CyberSANE has partnered once more with CS4CA, this time for their 24 hour Global Cyber Security Summit — CS4CA World, a unique initiative to revive and re-connect the industrial cyber security community world-wide.

## SPARTA Day and Brokerage Event

## April 12, 2021

CyberSANE participated in SPARTA's "SPARTA Day & Brokerage Event: We Are Connected" and was represented by Ana María Morales Perez and Jose Francisco Ruiz from ATOS.

## 2nd International Workshop on Cyber-Physical Security for CI Protection

### April 14, 2021

CyberSANE has joined other projects of the European Cluster for Securing Critical Infrastructures (ECSCI) in officially supporting the 2nd International Workshop on Cyber-Physical Security for Critical Infrastructures Protection (CPS4CIP 2021) which will take place virtually in late 2021.



# **Press & Other Content**

## FINSEC Project: CyberSANE joins the European Cluster for Securing Critical Infrastructures (ECSCI)

CyberSANE has recently become a new member of the ECSCI, bringing together more than 15 projects funded by the European Commission for enhancing the protection of Critical Infrastructures in Europe.

# European Commission: CyberSANE recognised by EU Innovation Radar

Some of the innovations developed during the project have been analysed and identified by the European Commissions Innovation Radar as well as the partners behind them deemed "Key Innovator's" in their development.

**Blog Post**: How does CyberSANE comply with the legal and ethical aspects for the protection of Critical Information Infrastructures (CIIs)?

By Ilaria Buri, KU Leuven <del>></del>

**Blog Post**: Web crawlers, data mining and extraction of knowledge from news articles and Dark Web

By Matej Kovačič, Jožef Stefan Institute. ≥

**Blog Post**: How to efficiently detect suspicious cyber activities? Encrypted Network Traffic Analysis and Transformation and Normalization techniques

By José Javier De Vicente Mohino, Atos and Eva Papadogiannaki, Forth <u>→</u>.

# **Scientific Publications**

#### "Model checking and machine learning techniques for HummingBad mobile malware detection and mitigation"

2020, Simulation Modelling Practice and Theory

Authors: Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone & Gigliola Vaglini – CNR, Italy ; University of Molise, Italy ; University of Sannio, Italy ; University of Pisa, Italy

#### "Towards an interpretable deep learning model for mobile malware detection and family identification"

2021, Computers & Security

Authors: Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo & Antonella Santone – CNR, Italy ; University of Molise, Italy.

#### "Neural Networks for Driver Behavior Analysis"

2021, Security and Trust in Next Generation Cyber-Physical Systems

Authors: Fabio Martinelli, Fiammetta Marulli, Francesco Mercaldo & Antonella Santone – CNR, Italy ; University of Campania, Italy ; University of Molise, Italy

#### "Driver Identification Through Formal Methods"

2021, IEEE Transactions on Intelligent Transportation Systems

Authors: Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone & Antonella Santone – CNR, Italy ; University of Molise, Italy ; University of Sannio, Italy

**CYBER**SANE

#### "Acceleration of Intrusion Detection in Encrypted Network Traffic Using Heterogeneous Hardware"

2021, IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD 2020

Authors: Eva Papadogiannaki & Sotiris Ioannidis – FORTH, Greece ; University of Crete, Greece

# **Meet the Partner**

## Foundation for Research and Technology -- Hellas (FORTH)



The Foundation for Research and Technology - Hellas (FORTH) was founded in 1983. It is one of the largest research centers in Greece with well-organized facilities, highly qualified personnel and a reputation as a top-level research institution worldwide.

FORTH conducts specialized scientific research in strategic high-added value sectors, focusing on interdisciplinary research and development (R&D) activities in areas of major scientific, societal and economic interest, such as: Lasers and Photonics, Microelectronics, Advanced Materials/Nanotechnology, Molecular Biology and Genetics, Biotechnology, Computer Science, Bioinformatics, Precision Medicine, Systems Biology, Robotics, Telecommunications, Applied and Computational Mathematics, Chemical Engineering Sciences, Energy, Environment, Human and Social Sciences, Astrophysics and Astronomy.

FORTH comprises 8 Research Institutes. Its headquarters and central administration are based in Heraklion, Crete, Greece.

In the context of the CyberSANE project, FORTH contributed to the cyber incident handling trend analysis in WP2. In WP3, FORTH led and delivered the Encrypted Network Traffic Analysis task and participated in the specification of Transformation and Normalization Analysis models. In WP5, FORTH led the development of the Dependency Evidence Chains Generation Algorithms and the Cyber Fusion Models. Details about the implementation of these two tasks are presented in the Deliverable 5.2. In WP6, FORTH contributed to the development of the Innovative Intelligence and Information Sharing models and the Trust, Security & Privacy mechanisms. In addition, FORTH's expertise in security and privacy enhanced the development of security and privacy modelling methods and techniques in WP7. FORTH continually disseminates project results through the publication of scientific articles and their presentation to scientific conferences, serves as Quality Manager and interacts with Standardization and Liaison bodies. Finally, FORTH's Encrypted Network Traffic Analysis tool, which introduces a new approach to effectively inspect encrypted network traffic now that the adoption of network encryption is constantly increasing, was highlighted by the European Commission's Innovation Radar.



**CYBER**SANE

Eva Papadogiannaki, PhD Candidate and Research Fellow



Christos Tzagkarakis, Research Associate



Manos Athanatos, Technical Project Manager











**KU LEUVEN** 



\*



**University of Brighton** 

Atos





SIDROCO



 $\mathbf{V}$ 

FUNDACIÓN VALENCIAPORT

Sphynx Technology Solutions

Ínría\_



lightsource bp

Klinikum Nürnberg

in	linkedin.com/company/cybersane-h220/
	twitter.com/CyberSANEH2020
►	youtube.com/channel/UCPq40hl019Ha8cEqZVVmbaQ
	www.cybersane-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 833683

