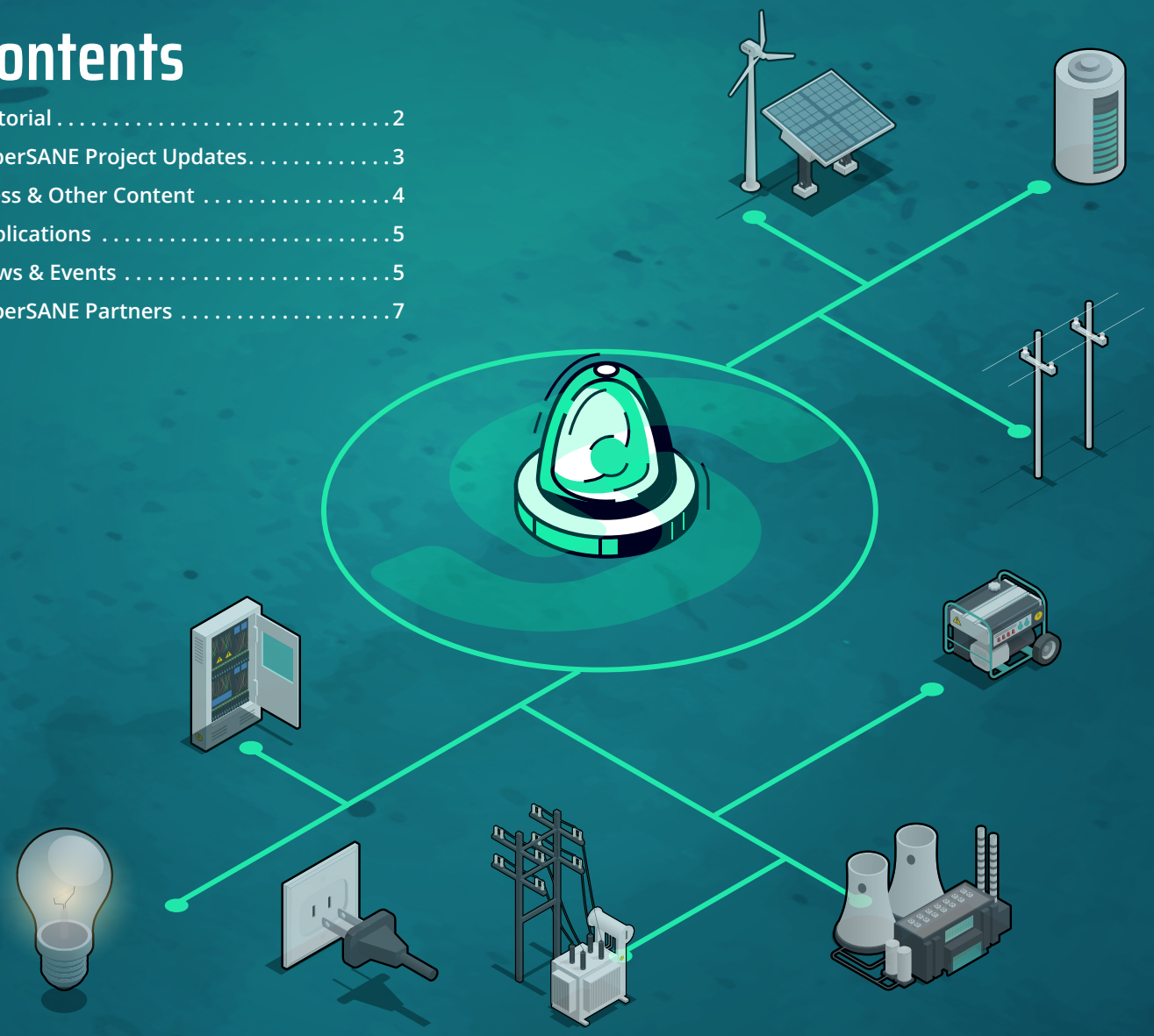
Newsletter #5 June 2022

CYBERSANE

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

Contents



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

Editorial

Welcome to the 5th edition of the CyberSANE Newsletter!

During the last month, the consortium has finished the implementation and integration phase of CyberSANE core components - LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet.

CyberSANE has started the validation and demonstration of its system in three different domains where cyber-attacks could have a severe impact: container cargo transport; solar energy production, storage, and distribution; and real-time patient monitoring and treatment.

Stay in touch on our social media channels to know more about the result of our pilots!

CyberSANE Project Updates

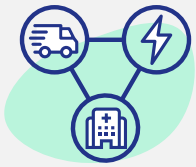
All CyberSANE work packages devoted to the development of the components have officially finished, but our team have been actively participating in the pilot preparation. CyberSANE components and tools are “live systems”, so we need to maintain data input all the time.

WP4 – DarkNet (Deep and Dark Web Mining and Intelligence)

The team is currently also finalizing the integration of EventRegistry into the CyberSANE platform.

The EventRegistry tool mines and analyses articles from news sites, social media and the World Wide Web in order to raise awareness about published articles, topics related to cyber security incidents in various sources. This can help the human operators to analyse the big picture of global malware and cybersecurity activities by providing analysis of media, news feeds and blog reporting. Automatic processing of a high volume of the collected information can be used to detect cybersecurity incidents, get an overview and insights of the techniques used by cybercriminals.

WP9 – Pilot Preparation and Operations



The last period has been very active in WP9 with the execution of the three project pilots. During that public events was demonstrated the different CyberSANE functionalities in three real scenarios.

The first pilot related to container cargo transportation was on 2nd February 2022. The focus of the scenario was a cyber-attack on one of Valenciaport’s platforms, used for sharing Verified Gross Mass amongst the ports community.

The second pilot related to solar energy production, storage and distribution was on 5th April 2022. It was focused on a variety of potential cyber-attack scenarios within a Solar Energy management platform, used for a number of digital services such as helping secure the electrical grid and reducing the cost of electricity.

The third pilot related to cyber-threat identification and communication in healthcare will take place on 1st July 2022. The focus of the scenario will be an attack to a hospital network through an infected notebook of an external service technician.

Press & Other Content

CyberSANE on Euradio

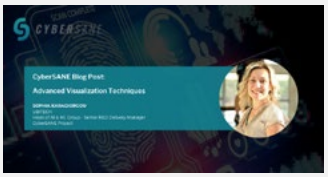
On the 28th January 2022, CyberSANE was presented on the French radio channel Euradio for Data Privacy Day.

Blog Post: Advanced Anomaly Detection capabilities and components of the CyberSANE System

We can define a cyberattack by a list of its attributes or in a negative way, saying what the cyberattack is not.

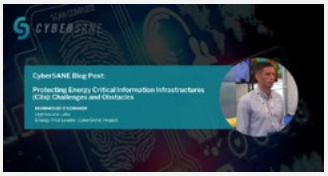
Blog Post: Protecting Transport CIIs: Challenges and Obstacles

During the design and preparation phase of the different attack scenarios for the transport pilot, the project partners identified several challenges.



Blog Post: Advanced Visualisation Techniques Visualisation Techniques in CyberSANE

Web crawlers are special applications used to create a copy of all the visited web pages for later processing.



Blog Post: Protecting Energy CIIs: Challenges & Obstacles

During the design and preparation phase of the different attack scenarios for the energy pilot, the project partners identified several challenges.

Blog Post: Using Deep learning for Anomaly Detection

The L-ADS (Live Anomaly Detection System) has the aim to classify in real time anomalous connections to a certain network. It is based on a deep learning algorithm called Auto-encoder. This kind of algorithm tries to learn about the normal behaviour of the network.

Publications

[AODV-Miner: Routage par Consensus Basé sur la Réputation](#).

Edward Staddon, Valeria Loscri, Nathalie Mitton AODV-Miner : Routage par Consensus Basé sur la Réputation - Archive ouverte HAL (archives-ouvertes.fr)

News & Events

CyberSANE Transport Pilot Case Study

2 February 2022, Virtual

CyberSANE held the first Pilot Case Study, organised by Fundación Valenciaport. This pilot revolved around testing and validating the CyberSANE System, in the scope of a cyber-attack scenario on one of Valenciaport's platforms, used for sharing Verified Gross Mass amongst the ports community.

2nd Joint Workshop – Dynamic Countering of Cyber-Attacks Projects | Achievements and Standardisation

8 February 2022, Virtual

This Workshop was a follow up to the first edition back in 2021 and joined the same projects from the SU-ICT-01-2018 H2020 call: C4IIoT, CARAMEL, GUARD, SAPPAN, SIMARGL and SOCCRATES. The projects shared their overall progress, created synergies and set a common ground for standardisation activities.This time the event was open to the public and counted within the support of the Fiware Foundation.

CyberSANE Energy Pilot Case Study

5 April 2022, Virtual

CyberSANE hosted its 2nd Pilot Case Study, organised by Lightsource Labs. This pilot demonstrated, tested and validated the CyberSANE System, involving Lightsource Labs showcasing a variety of potential cyber-attack scenarios within their Solar Energy management platform, used for a number of digital services such as helping secure the electrical grid and reducing the cost of electricity.

CyberSANE at the 2nd ECSCI Workshop on Critical Infrastructure Protection

27-29 April 2022, Virtual

This workshop presented the different approaches on integrated cyber and physical security in different industrial sectors, such as energy, transport, drinking and waste water, health, digital infrastructure, banking and financial market, space and public administration. Different projects of the ECSCI cluster Presented their outcomes, discussing the technical, ethical and societal aspects and the underlying technologies. The workshop included keynote speeches, 23 projects presentations, roundtable and panel discussions, and thematic presentations.

CyberSANE at GDR RSD 2022

27th and 28th April 2022, Paris

The GdR Networking and Distributed Systems aims to contribute to the scientific animation, structuring, revitalization, promotion of knowledge and synergy of these two founding research areas of the great advances and innovations in the field of Sciences and Technologies of Information and Communication (STIC).

CyberSANE at CoRes 2022

30-31 May 2022, Saint-Rémy-Lès-Chevreuse, France

The 7th Francophone Meeting on the Design of Protocols, Performance Evaluation and Experimentation of Communication Networks (CoRes 2022) is a conference to bring together the French-speaking community around issues related to the design, modelling, performance evaluation and experimentation of communication networks. It is co-organized with Algotel 2022, which will offer the possibility of having, within the same place, close communities who do not often have the opportunity to meet

CyberSANE Partners

UBITECH

UBITECH is a leading, highly innovative software house, systems integrator and technology provider, established to provide leading edge intelligent technical solutions and consulting services to businesses, organizations and government in order to allow the efficient and effective secure access and communication with various heterogeneous information resources and services, anytime and anywhere. UBITECH enables real-time valid information processing and decision-making, the realization of intelligent business environments, and B2B and B2C transactions by providing high added-value business –oriented and –based solutions. UBITECH LIMITED is the youngest member of UBITECH Group that has been established in 2005, concentrated initially in the Balkan market and acquiring several EC and national grants for novel R&D initiatives.

Sophia Karagiorgou

Currently, UBITECH Group has extended its operations with targeted international activities through its subsidiaries, representation offices, business partners and affiliated companies in Limassol (UBITECH LIMITED), Madrid (Business Development Office), Buenos Aires (UBITECH SRL targeting mainly Argentina, Paraguay, Uruguay and Bolivia) and Guayaquil (Business Partner and Representation Office for Ecuador and Panama), concentrating mainly in the Spanish-speaking countries of Central and Latin America.

Technology innovation constitutes the lifeblood of UBITECH. We are continuously seeking and validating new, emerging technologies, developing new ideas, concepts and solutions, and improving existing software applications and products for vertical markets or for addressing specific end-users' needs. UBITECH R&D team – that spans across all group's companies, collaborating and exchanging experiences and technological know-how, reinforcing the group's research capacity – is engaged in developing, integrating, deploying, piloting, demonstrating and evaluating innovative technologies, utilities, features and processes, transferring technological know-how to end-user organizations and adapting breakthrough solutions to end-users' demands. UBITECH R&D team participates in large, multidisciplinary consortiums in complex and highly-innovative projects, including experts from universities, research institutes and industry across the enlarged Europe, which partner to provide research, technology integration and skilled project management. UBITECH R&D team members can demonstrate strong involvement in EC and National co-funded research programmes, though the design, development and implementation of research and technological development instruments.

Based on group's strategy for research and innovation, every group member participates actively into the research and development of cutting-edge tools and methodologies to improve the solutions and services of the group. Thus, UBITECH LIMITED (Cyprus) researchers, depending on their expertise and the local exploitation potential, perform applied research in the areas of Cloud Computing, Software and Services; 5G Technologies; Digital Security, Big Data and Analytics; Cyber-Physical Systems and Internet of Things; Energy Efficiency; Factories of the Future; e/m-Health. UBITECH has a strong a focus on the integration and interoperability of information technology solutions and applies its research results to solve problems in various application-oriented projects in several domains (included but not limited to Life Sciences and e-Health, Ambient Assisted and Independent Living, e-Government and Policy Modelling, Lifelong Education and Technology-enhanced Learning, e-Culture, e-Business and Networked Enterprise, Digital Factories, Security and Environmental Management).

UBITECH contributes to all activities with regard to the implementation of all main components - LiveNet (WP3), DarkNet (WP4) HybridNet (WP5), ShareNet (WP6) and PrivacyNet (WP7) - of the CyberSANE system as well as in the development of the visualization techniques (WP8). In addition, UBITECH is heavily involved in the system integration and testing (WP8) as well as in the deployment, configuration, operation and evaluation of the integrated CyberSANE system at the pilot sites (WP9 & WP10). Finally, UBITECH works towards the dissemination and exploitation of the project's outcomes (WP11).

JSI

Jožef Stefan Institute (JSI) is the leading research institution for natural sciences in Slovenia having over 900 researchers within 27 departments working in the areas of computer science, physics, and chemistry and biology. Artificial Intelligence Laboratory (AILAB), having approx. 50 researchers, is one of the largest European research groups working in the areas of machine learning, data mining, language technologies, semantic technologies and sensor networks. The key research direction is combining modern statistical data analytic techniques with more semantic/logic based knowledge representations and reasoning techniques with the purpose to progress in solving complex problems such as text understanding, large scale probabilistic reasoning, building broad coverage knowledge bases, and dealing with scale.

AILAB is working for a decade in various areas of implementing AI to real cases. This include among others cognitive freight transport, intelligent mobility, energy efficiency, intelligent municipalities and smart cities, factories of the future and proactive production systems, eLearning and personalization, language technologies and automatic translation as well as government transparency and cyber security.

Besides research projects, AILAB is also involved in several commercial projects with companies like Accenture Labs, Bloomberg, British Telecom, Google Labs, Microsoft Research, New York Times, Siemens, Wikipedia, AdriaMobil. The work here is combined with set of AILAB spin-out companies Quintlligence, Eventregistry, Qlector, SolvesAll, LiveNetLife and BlueEye.

JSI as a research institute is having a key role in the design of the CyberSANE concept, in particular it is the main contributor of the DarkNet components (WP4) of the CyberSANE system, based on its expertise from previous approaches and on the tools the institute has already developed. As such, JSI is leading WP4 and specially Task T4.3 that has to do with the Social media crawling and data aggregation, and is also leading the specification of the Data Collection, Migration, Harmonisation and Linkage Algorithms (Task T4.4) and the Data Analytics and Business Intelligence models (Task T4.5), also contributing to the integration of the Deep and Dark Web mining and intelligence (DarkNet) Component under Task T4.6.

Matej Kovačič

SID

Sidroco Holdings Ltd (SID) is a creative SME focusing on Research, Development and Inspiration. SID designs, develops and implements novel and innovative products, frameworks and tools. Together with these innovative solutions, SID also supports techo-economic analysis, business models and advanced market analysis using brand reputation tools. SID is able to support a variety of research solutions and integrated products in multiple domains such as network and system security, modelling and simulation, optimization, visualization, machine learning solutions, risk analysis and assessment, market analysis and business modelling. SID develops and integrates smart honeypots for attracting and capturing attack traces and logs, while it develops a penetration testing suite for providing a detailed security and privacy analysis in any environment.

SID has been working in developing Visualize everything as a service with the SiVi© tool in integrating 5G services in a simple toolbox. Also, SID has been working in developing SiBR© solution in acquiring the social sentiment analysis

Antonios Sarigiannidis

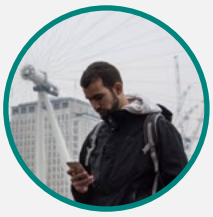
Anna Triantafyllou

in modern social media. Also, SID has been participating in several national and European projects by contributing to technical and financial reports, the development of advanced SIEM tools with visual-assisted techniques and visualisations, performing extensive penetration testing, integrating security components and promoting project achievements through publications at high quality ranked international conferences and journals.

SID is providing the SiVi Tool, which is a human-interactive visual-based anomaly detection system that is capable of monitoring and promptly detecting several devastating forms of security attacks, including wormhole attacks, selective forwarding attacks, Sybil attacks, hello flood attacks and jamming attacks. Based on a rigorous, radial visualisation design,SiVi Tool can expose adversaries conducting one or multiple concurrent attacks against IoT-enabled infrastructure. SiVi Tool visual and anomaly detection efficacy in exposing complex security threats is demonstrated through a number of simulated attack scenarios.

In this context, SID is leading research provider for the project, through the contribution of a range of research results for increasing the handling of cyber-security incidents in WP3 and WP5.

Anastasios Lytos



Paris-Alexandros Karypidis

UoB

University of Brighton

The University of Brighton (UoB) is a community of 21,300 students and 2,600 staff based on five campuses in Brighton, Eastbourne and Hastings. We have one of the best teaching quality ratings in the UK and a strong reputation for quality research. We pride ourselves on pioneering new approaches with innovative and relevant research that addresses current issues and challenges. Research in Computing, Engineering and Mathematics (CEM) aims to deliver a high quality foundation for the effective design, application and use of technology to advance social, cultural and economic development. Our wide range of research applications is underpinned by a focus on impact delivery and validated in close collaboration with end-users as well as the national framework for the assessment for research quality. The Computing Division of CEM has research consolidated into the Centre for Secure, Intelligent and Usable Systems (CSIUS). CSIUS focuses on both theoretical and practical research in computer science challenges related to security, intelligence and usability of software systems.

Haris Mouratidis

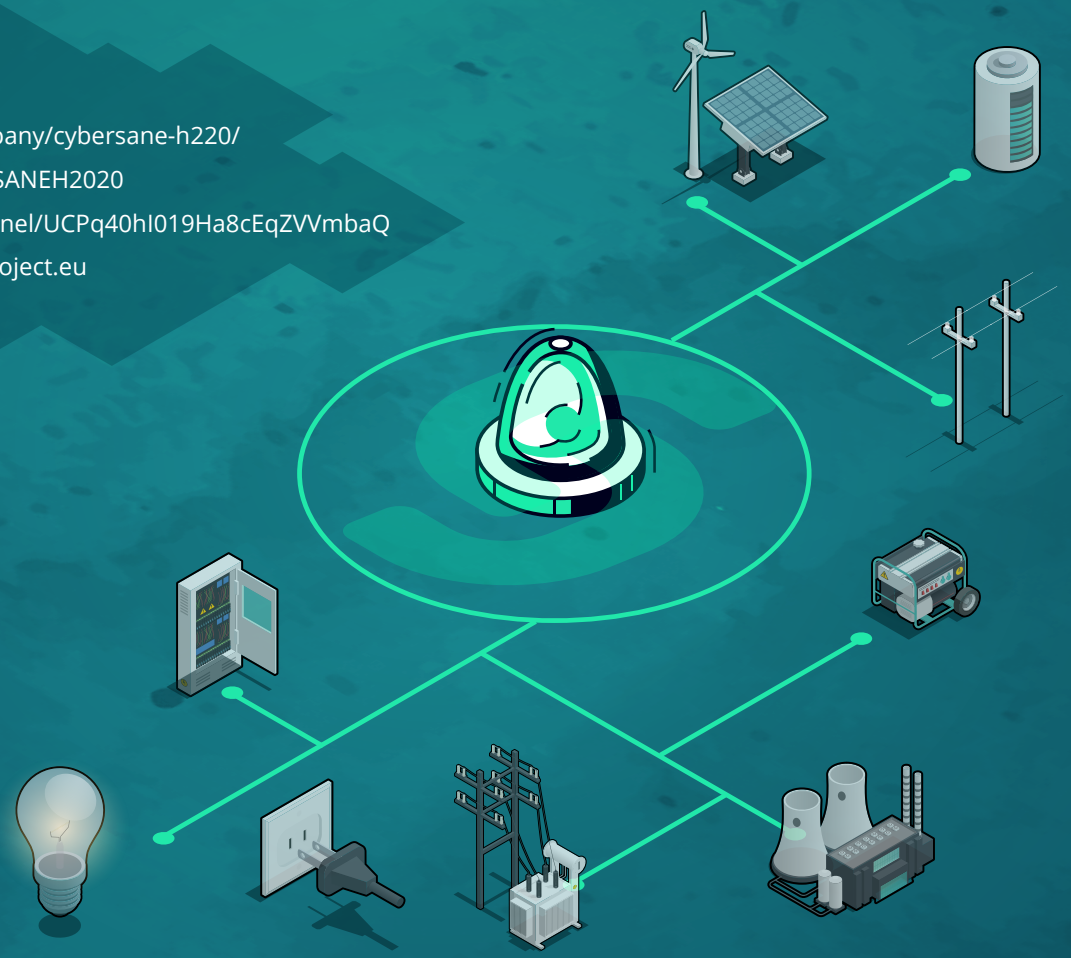
The UoB has long experience and participation in EU funded projects.

The Security theme of the Centre for Secure, Intelligent and Usable Systems (CSIUS) produces work in the intersection of software engineering, security engineering and risk management. We have pioneered work in ontologies, languages, models, processes, methodologies and automated testing and optimisation techniques that consider security, risk, trust and privacy as an integral aspect of the software systems development process.

UoB contributes mostly to WP7 because of its expertise and experience in security and privacy enabling technologies. In particular, UoB uses its expertise in security and privacy to lead the development of security and privacy modelling methods and techniques (T7.2 Security and Privacy Modelling).

CYBERSANE

linkedin.com/company/cybersane-h220/
twitter.com/CyberSANEH2020
youtube.com/channel/UCPq40hI019Ha8cEqZVVmbaQ
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