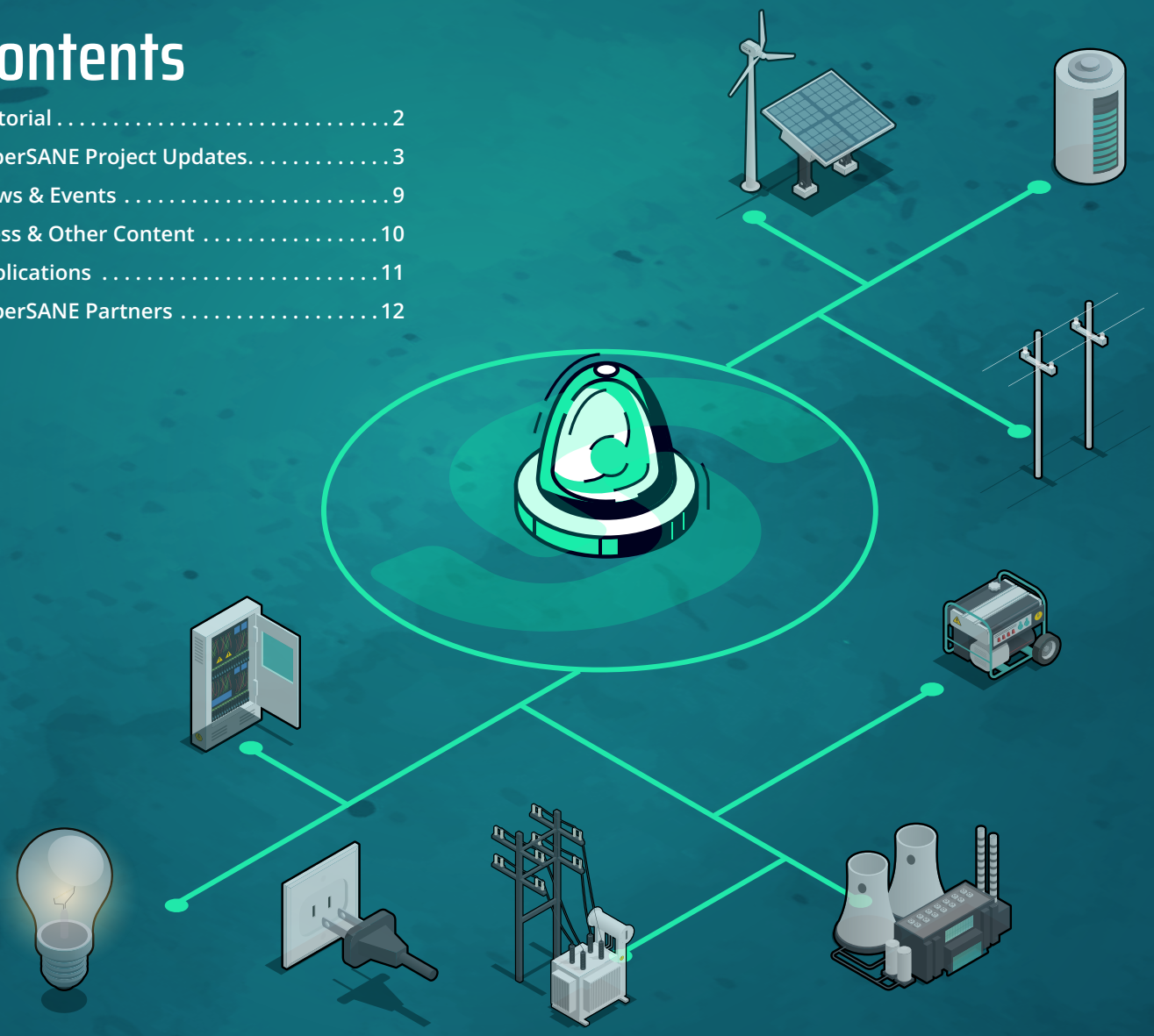
Newsletter #4 January 2022

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 4th edition of the CyberSANE Newsletter!

Since the start of the project in September 2019, the consortium has been working on requirements elicitation and the design of the architecture of the System addressing technical and cognitive challenges against cyberattacks on CIIs. CyberSANE architecture implements all phases of the Cyber incident handling lifecycle, increasing the agility of security professionals and experts, encouraging continuous learning, through various layers which are mainly realized in the main CyberSANE web application.

After ending the implementation and integration phase of the six core components - LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet – CyberSANE project will start in 2022 with 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.

Find in this edition everything you need to know about the CyberSANE system, the features and benefits provided by each one of its components.

Stay in touch on our social media channels to know more about piloting activities.

CyberSANE Project Updates

WP3 – LiveNet (Live Security Monitoring & Analysis)

For WP3, the objectives have been met, since almost all the tasks are finished and the objectives set in the description are being met, with more than 6 techniques implemented which are: encrypted network traffic analysis, event correlation, intrusion detection, network traffic monitoring, log extraction (transformation), log normalization, signature mining. The enhancements have been described in D3.2 and D3.3.

Live Security Monitoring Analysis: Both the architecture and the definition of LiveNet services and dashboards are done. Regarding Cybersecurity Sensors (LiveNet monitoring), we have listed NIDS, Antivirus, Firewall, ICS sensors (DICOM),Operating system logs

Encrypted Network Analysis: We performed literature examination and signature generation. After that, a setup of a virtual environment for attack generation has been produced. With malicious traffic collection, we gathered ground-truth dataset analysis, performing signature generation (pattern mining for automation). The integration into FORTH's intrusion detection system produced resulted signatures (attack patterns) and intrusion alerts (security incidents) transmitted to the CyberSANE platform.

Transformation and Normalization analysis: We choose ECS (Elastic Common Schema) as the normalization model. The identified advantages of normalization are these:

- ☑ Reducing the amount of data to be processed and, therefore, the time required.
- ☑ Funnelling data to the output.
- ☑ Producing an expected, structured output.
- ☑ Avoiding data confusion and disruption
- ☑ All technical partners were aligned with ECS normalization
- ☑ **LiveNet Component Integration**: The LiveNET architecture was completed, including communication and interconnection, and being compliant with ECS - normalization. Finally, the integration with CyberSANE core included integration with:
  - Security Incidents
  - Alerts & Notifications

Pilot tasks related to the LiveNet (currently in progress):

- ☑ Finalizing and testing the integration of GLORIA as a LiveNet tool to send information about the solution.
- ☑ Selecting and identifying signatures and messages to be representative and real enough for the Pilot Scenarios (Exploit, Email with malware, File deletion audit, ...).
- ☑ Currently, finalizing integration development and in the following weeks, we will deploy in the mentioned pilot environment, running the pilot use cases (through GLORIA detection rules).
- ☑ Finally, connecting to the CyberSANE core (HTTP POST) to complete the pilot preparation.

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

DarkNet component of the CyberSANE platform is a software solution for searching and analysing threat actor communications in dark web communities and a solution for automatic monitoring and aggregating unstructured data in media articles blog posts and social media. Our solution is enabling cross-lingual analysis of the crawled content and provides business intelligence. This helps end-users to get the big picture of global cybercrime and cybersecurity activities and to raise awareness about cyber incidents to the end-users.

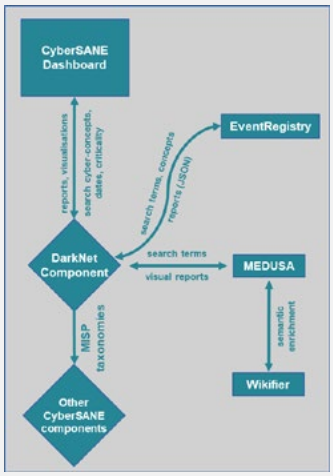


Figure: The DarkNet Component and its interoperation within the CyberSANE Platform.

The work package developing the DarkNet component has finished in 2021 and in the final deliverable, we have described functionalities, specifications and configuration details of our tools for performing deep web threat intelligence and open web threat intelligence.

Underlying tools are offering Application Programming Interfaces (APIs) adopting open interoperability standards, which enables the DarkNet services to interact with other CyberSANE components and the whole platform. That enables the DarkNet component to serve as the Threat Web Intelligence reporting mechanism to the CyberSANE Platform.

DarkNet component provides deep web threat intelligence and open web threat intelligence. These functionalities are the result of two core tools – **MEDUSA** and **EventRegistry**.

The **MEDUSA** tool collects, mines and analyses content from the dark web, marketplaces selling illegally personal data, sites about breached data and pawned email accounts to further identify cyber incidents related to the rumour and the corporate identity of an organization, employees' breached email accounts and cyber-attacks (i.e., DDoS, malware, trojan, etc.).

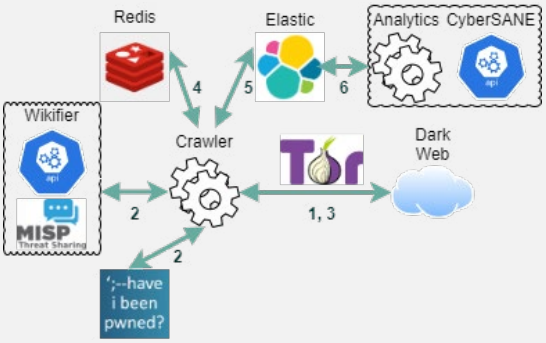


Figure: The MEDUSA Architecture.

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.

During the project, we enhanced the functionality of the Event Registry and the MEDUSA tools, which are now integrated into the CyberSANE platform through APIs. We focused on collecting and storing the collected data in a highly scalable storage framework for further mining. The collected data are then feeding machine learning algorithms for text classification, clustering and graph analytics. The collected and curated data are stored in the Elastic search and through the Elastic Common Schema are made available to the ShareNet component for advanced cyber incidents awareness among different users and entities.

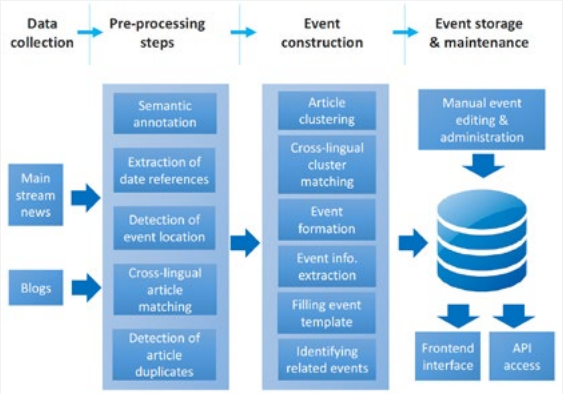


Figure: The EventRegistry Architecture.

We are collecting more than 2 GB of data per day (around 1.2 GB from EventRegistry and more than 20.000 documents from MEDUSA), and these data are further enriched and analysed feeding other services and tools. From these data, we are extracting useful information that can be used to report about illegal trading of breached data in marketplaces, blacklisted email servers and news about the corporate rumour of Critical Infrastructure owners found in worldwide and dark web sites.

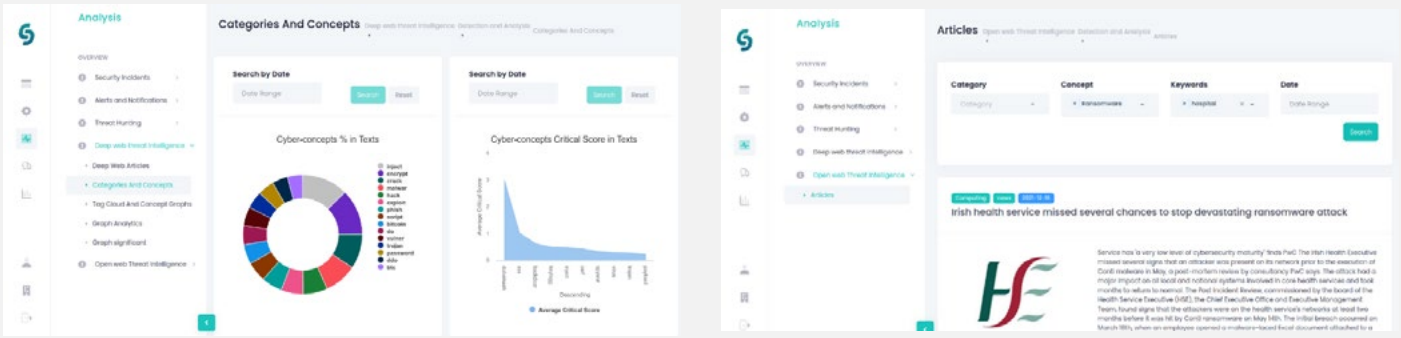


Figure: DarkNet component integration into the CyberSANE platform - deep web threat intelligence.

WP5 – HybridNet (Data Fusion, Risk Evaluation, and Event Management)

In the scope of WP5, the design, development and integration of the HybridNet has reached the last stage of development of the different tools and are already testing them into the use cases in order to satisfy the needs of the different critical infrastructures.

Therefore, in the initial phase of the project, we worked on identifying how to extend and improve the solutions we had for the HybridNet. For this, we used two different approaches: analysis of the state of the art and needs from the use case partners.

The analysis of the state of the art focused on machine learning capabilities. Among other capabilities, we worked on improving the algorithms we have for detecting attacks and reducing the number of false positives/negatives. This work was done in the three initial tools of anomaly detection we have in the project and the initial results were very satisfactory in terms of performance and results.

Additionally, we worked in extending these tools and the ones for simulation of attacks with the information of the use cases. For this activity, we had specific meetings with them in order to explain what the tools already provided and what the tools could provide to them. This was a very positive meeting and gave us many ideas and research and development paths so we could adapt our tools to their needs. Also, this created future pathways that we want to explore after the project ends together with integration with other tools so the experience in this area was very satisfactory.

Following the process of development, we started integrating the tools into the CyberSANE platform and the use cases. The reasoning for this parallel work was to take the chance to start refining and testing the tools while working in their technology integration in the common platform so that way we could provide more experimented and mature versions of the tools.

Currently, we are in the final phase of the integration of the tools in the common platform and plan to start validating the HybridNet in the use cases, but with the platform as a whole in order to adapt the different components and functionalities. The three use cases will be able to test this layer and we will check the fulfilment of the requirements they identified so we can have a clear idea of the level of completion and how to continue extending and adding new functionalities.

WP6 – ShareNet (Intelligence, Information Sharing and Dissemination)

The ShareNet component of the CyberSANE platform offers data-sharing infrastructure allowing security professionals to exchange cyber incidents information with third parties securely.

The ShareNet is a software solution that enables control over data access and usage according to Data Sharing Agreements (DSAs), which specify a set of security policies and organizations involved in the sharing process. This helps security professionals to specify conditions under which particular users can access and use information, and Data Manipulation Operations (DMOs) to be executed on information to protect sensitive data.

The work package related to the ShareNet component development has finished in 2021 and its final deliverable provides main functionalities, specification and configuration details.

ShareNet tools offer multiple Application Programming Interfaces (APIs) utilizing open interoperability standards to allow ShareNet to interact with the CyberSANE platform and other components. In this way, ShareNet serves as a secure information-sharing mechanism to the CyberSANE Platform also supporting the enforcement of data anonymisation functions.

ShareNet component provides secure information sharing and security policy management functionalities. Two core subcomponents, namely **DSA Manager** and **Information Sharing Infrastructure**, realize those functionalities.

The DSA Manager supports security professionals with the policy management functionalities allowing them to define, store, edit and delete policies defined through the DSAs. Then, data owners or other stakeholders can attach those DSAs to a dataset in order to regulate access to that data. Furthermore, as already mentioned security professionals can specify particular DMOs to be executed by the system to prevent privacy. For this reason, ShareNet uses a set of PrivacyNet APIs to manipulate, i.e., anonymise, particular fields of data.

Information Sharing Infrastructure of the ShareNet component supports security professionals with data sharing functionalities allowing them to share data securely according to policies specified in DSAs.

Furthermore, the ShareNet system may invoke PrivacyNet APIs to manipulate data if certain conditions are met. In this way, data owners may request a system to share only manipulated, e.g., anonymised version of data with third parties, while the original data will be shared only with partners properly specified in the corresponding DSA.

During the project, we enhanced functionalities of the ShareNet tools, which are integrated into the CyberSANE core platform through the set of APIs. We focused on information sharing and storing functionalities to provide a more secure and general approach for data exchange under restrictions specified in security policies. We have also integrated additional tools that validate information quality based on multiple criteria in order to compute the trust score for each stakeholder and consider this parameter during the policy evaluation process.

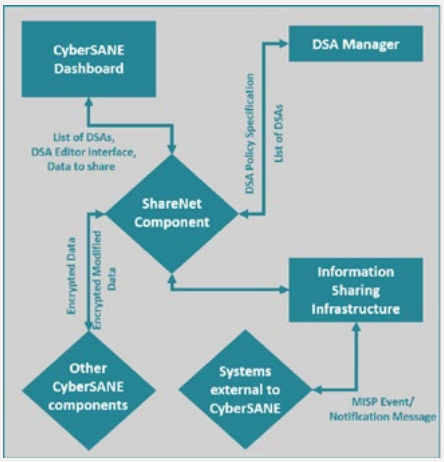


Figure 1: The ShareNet component and its interaction with CyberSANE Platform

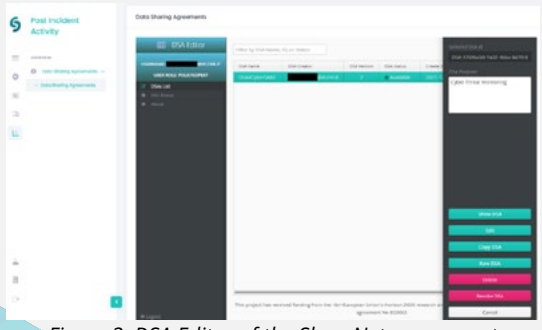


Figure 2: DSA Editor of the ShareNet component integrated into CyberSANE platform

WP8 – CyberSANE System

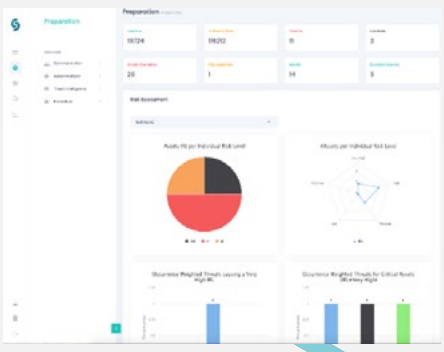
CyberSANE officially released the first prototype of the CyberSANE platform, which realizes the proper implementation of five main and core structural elements/components:

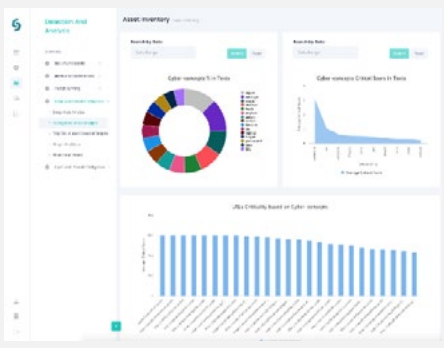
- The **Live Security Monitoring and Analysis (LiveNet)**, which is capable of preventing and detecting threats, providing to security professionals insights and a track record of the activities within their Information Technology environment.
- The **Deep and Dark Web Mining and Intelligence (DarkNet)**, which allows the exploitation and analysis of security risks and threats related information from the deep and dark Web
- The **Data Fusion, Risk Evaluation and Event Management (HybridNet)**, which provides the intelligence needed to perform effective and efficient analysis of security events
- The **Intelligence and Information Sharing and Dissemination (ShareNet),** which provides the necessary threat intelligence and information sharing capabilities of the critical infrastructure with other external parties that the Critical Infrastructure would like to involve, allowing them to determine the trustworthiness of each information source.
- The **Privacy & Data Protection (PrivacyNet) Orchestrator**, which is responsible for managing and orchestrating the application of the required privacy mechanisms, maximizing achievable levels of confidentiality and data protection.

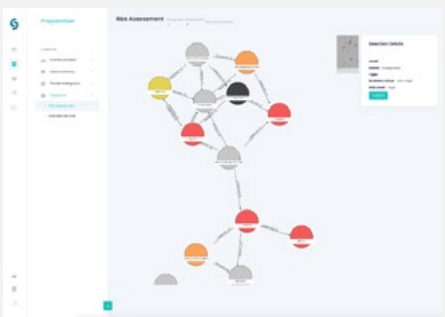
All CyberSANE structural elements provide a set of services and functionalities grouped in four different phases:

- The **Preparation phase**, which emphasizes the actions required to be taken from an organization in order to be ready to respond to incidents but also to prevent from incidents by ensuring that systems, networks, and applications are sufficiently secure.
- The **Detection and Analysis** phase, the main purpose of which is to determine whether the incident is really occurring and analyze its nature.
- The **Containment, Eradication and Recovery** phase, in which the incident response team tries to contain the incident and, if necessary, recover from it (restore any affected resources, data and/or processes).
- The **Post Incident Activity** phase, in which Security Experts attempt to determine specifically what happened, why it happened, and what the organization can do to keep it from happening again.

All four phases are the main phases that the NIST Computer Security Incident Handling Guide introduces, which assists organizations in establishing computer security incident response capabilities and handling incidents efficiently and effectively. Specifically, it provides guidelines for incident handling, particularly for analyzing incident-related data and determining the appropriate response to each incident.







WP9 – CyberSANE Pilots

In the last months, the CyberSANE partners have been working hard in the three pilot preparation, in order to test and verify the functionalities of the CyberSANE platform in different fields. For each of them, we have defined step by step what is going to happen during the pilot execution and the CyberSANE components which will detect the cyber-attack. In addition, we have deployed the necessary infrastructure for the first pilot.

All the information related to the pilot preparation and the scenarios designed can be found in the deliverable D9.1, which was delivered in September.

In the coming months, we will run the three pilots, starting with the Container cargo transportation pilot in January. The proposed date for the Solar Energy production, storage and distribution pilot in March. Finally, the Cyber-threat identification and communication in the healthcare pilot will be in May.

Read more about this on the Blog Post - CyberSANE Pilot Scenarios: Transportation, Energy & Healthcare.

CyberSANE Transport Pilot Case Study

Feb 2, 2022 - 10:00 - 12:30 CET

CyberSANE will hold the first Pilot Case Study, organised by Fundación Valenciaport. This event will take place online via Teams.

This pilot revolves 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.

Participation in this event is free of charge, however, registration is required.

Click here to see the agenda and register.

News & Events

CyberSANE at ARES 2021

17 Aug 2021

From the 17th to the 20th August 2021, CyberSANE will participate in the all digital 16th International Conference on Availability, Reliability and Security (ARES 2021).

During this event, CyberSANE will be presented by our very own Quality Assurance Manager, Manos Athanatos from FORTH. The presentation will take place on the 17th August at 15:30! ➔

CyberSANE at CyberHOT Summer School 2021

27 Sep 2021

On the 27th and 28th September 2021, the CyberSANE participated in the CyberHOT Summer School.

Furthermore, CyberSANE also sponsored this event providing both content and speakers, thus supporting the sharing of cyber security related knowledge, helping them to respond and combat anything that they may encounter.

Two of our partners from FORTH, Eva Papadogiannaki and Manos Athanatos, attended the event and took a moment to present CyberSANE to the other participants. ➔

CyberSANE at the Concordia Open Door Event 2021

20 Oct 2021 | Virtual

The 20th and 21st October 2021, CyberSANE will once again participate in CONCORDIA's Open Door 2021 virtual event.

CyberSANE will hold a virtual-exhibitor stand to present the project to industry specialists and other event participants. ➔

CyberSANE at the Cyber Ireland National Conference 2021

21 Oct 2021

On the 21st October 2021, CyberSANE will participate in the Cyber Ireland National Conference (CINC).

During this event we will be represented by Diarmuid O Connor from Lightsource Labs. ➔

Press & Other Content

Press release: CyberSANE project successfully ends its implementation, integration, testing and pilot set-up phase

Starting 2022, CyberSANE will focus on 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. →

Blog post: Intelligence and Information Sharing models

During the first half of 2021, WP6 (lead by CNR) has been continuing work on the ShareNET system. The team developed and integrated new components to enable secure and automated Cyber Threat Intelligence (CTI) sharing with third parties and an external Threat Intelligence Sharing Platform (TISP). →

Blog post: Why visualization systems are important within the cybersecurity domain?

To enhance the decision support actions, interpret, and explain large volumes of data, a security analyst will leverage the functionalities of a Visual Intrusion Detection System (V-IDS). These systems will offer helpful insights from complex logs, provide a good overview of the entire system and they are often used as an extra anomaly detection mechanism. →

Blog post: CyberSANE Pilot Scenarios: Transportation, Energy & Healthcare

The CyberSANE project has developed an advanced, configurable and adaptable, security and privacy incident handling systems with the aim to improve, intensify and coordinate the overall security efforts for the effective and efficient identification of threats, and the investigation, mitigation and reporting of multi-dimensional attacks. In order to test and verify the developed functionalities in different domains, three pilots have been designed to gather feedback. →

Publications

A Survey on Encrypted Network Traffic Analysis Applications, Techniques, and Countermeasures

Eva Papadogiannaki, Sotiris Ioannidis. →

Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey

Edward Staddon, Valeria Loscri, Nathalie Mitton. →

On Strengthening SMEs and MEs Threat Intelligence and Awareness by Identifying Data Breaches, Stolen Credentials and Illegal Activities on the Dark Web

George Pantelis, Petros Petrou, Sophia Karagiorgou, Dimitrios Alexandrou. →

This Sneaky Piggy Went to the Android Ad Market: Misusing Mobile Sensors for Stealthy Data Exfiltration

Michalis Diamantaris, Serafeim Moustakas, Lichao Sun, Sotiris Ioannidis, Jason Polakis. →

CyberSANE Partners

KU Leuven

KU Leuven Interdisciplinary Centre for Information Technology and Intellectual Property (CiTiP) is a research centre at the Faculty of Law of KU Leuven, with currently a staff of over 60 researchers specialized in legal and ethical aspects of IT technology and innovation. CiTiP is among the founding members of the Leuven Center on Information and Communication Technology (LICT) and of the Flemish digital research and incubation center iMinds (www.iminds.be) that recently merged with imec, a world-leading research and innovation hub in nano-electronics and digital technologies (www.imec.be).

Prof. Dr. Anton Vedder, Professor of Law & IT (Principal Investigator)

CiTiP's staff has access to leading technical experts in Flanders via its affiliation to LICT, imec and steady relationships with many science and technology departments at KU Leuven. CiTiP has a solid track record as an ethical-legal partner in large international and interdisciplinary research projects and is internationally renowned for its expertise in the areas of data protection, privacy and information security law, new media and communications law, information rights management, and intellectual property rights. It is currently involved in more than 70 research projects, funded by the European Union (EU) (FP7 and Horizon 2020), the Belgian Research Council, FWO, and various other parties. Detailed information can be found on http://www.law.kuleuven.be/citip/.

Dr. Ana Maria Corrêa, Postdoctoral researcher

In the context of the CyberSANE project, CiTiP provides legal and ethical expertise to the consortium to ensure that the development and use of the CyberSANE solution complies with the relevant requirements. As part of the work accomplished in WP2, CiTiP delivered the D2.2 which present the legal and ethical requirements relevant to the CyberSANE platform. CiTiP's work has put focus on the fundamental rights potentially impacted by the use of the platform, the EU framework on data protection, network information system security, critical infrastructures, cybercrime and the ethical requirements for trustworthy artificial intelligence.

Burcu Yaşar, Legal researcher

In WP10, CiTiP works in close collaboration with other partners to evaluate whether the platform complies with the identified requirements and policy guidelines. Moreover, CiTiP provides its expertise to the consortium to ensure the ethical conduct in CyberSANE research. In this regard, CiTiP has worked on the deliverable D1.2 Ethics, Privacy and Security Management Plan, provided supporting documents and participated in relevant meetings. Finally, CiTiP contributes to the WP11 by contributing to the dissemination activities and engagement with standardization bodies. A brief overview of CiTiP's research can be found on https://www.cybersane-project.eu/legal-ethical-aspects-cii-protection/.

Sphynx Technology Solutions AG - Switzerland (STS)

STS offers products and solutions, and consulting services, in the areas of cyber intelligence, analytics, incident response, assurance, and certification. Through a variety of products, STS can provide customised and continuous security and privacy assessment solutions, covering the full range of socio-technical aspects of a modern enterprise, for internal risk management and/or external security audit and certification.

All these solutions are based on a novel Security and Privacy Assurance (S&P) and platform with advanced analytics and cyber intelligence features for enterprise security assurance. By doing so, the set-up of security assessments based on industrial and international standards (e.g., cloud, network, smart metering standards) is made feasible, leveraging as well external tools including threat analysis, vulnerability and penetration testing, continuous monitoring at all levels of the enterprise system implementation stack, sophisticated event processing and anomaly pattern detection.

STS also offers a Security Operation Centres (SOC) service which extends the SA service to a managed form, including all the security operation, consultancy and technology maintenance services. At its core, the SOC service involves the analysis and filtering of the automated security assessments of the SA service by expert security engineers and the provision of vetted and prioritised information to them along with expert recommendations for and overseeing of incident responses.

Moreover, STS supports Incident Response (IR) playbooks, providing automation on incident responding as well as the compliance of those playbooks to standards providing the capability to easily exchange such playbooks. It is also worth mentioning that both S&P and SOC services can be further extended with cyber-security training programmes (Cyber Range/CR programmes). The provision of CR programmes enables the development of incident prevention and response skills for an organisation's personnel, as well as training towards different security certifications at personal and/or organisational level. CR programmes cover different threat actors, scenarios, incidents, and are based on emulated, simulated, and hybrid replicas of client systems. Under the advanced levels of offering the service, CR programmes are also be tailored to the needs of the individual clients.

In the context of CyberSANE project, STS contributes to several WPs of the project and acts as the Risk Manager, leading T1.5 and the effort of identifying and monitoring the most relevant risks and opportunities that may arise during the implementation of the project. In WP2, STS contributed to addressing platform's technical specifications and reviewing the most prominent EDR solutions which resemble CyberSANE's expected functionalities, while in WP3, STS provided the key challenges met in today's transport Critical Information Infrastructures (CIIs) and analysed the most used transformation and normalization techniques. In WP4, STS introduced the MISP Threat Intelligence Sharing Platform capabilities in terms of event types, taxonomies, and galaxies. In WP5, STS led the effort to create a report on the state-of-the-art prevention and response to advanced threats methodologies, analysing the outcomes as well and proposing a set of enhancements to consortium tools for the development of CyberSANE's dependency evidence chain algorithms and Cyber Fusion Models. In WP6, STS coordinated the production of the specification required in platform's Intelligence and Information Sharing Models, while in WP7, STS contributed to the specification of the homomorphic encryption schemes and blockchain technologies. In WP8 and WP9, STS assists to the integration and validation of the CyberSANE system by providing the appropriate evaluation methodologies and tools in the context of WP10. Last but not least, STS also participates in WP11 by disseminating, communicating, and reporting its exploitation and business plans for CyberSANE project.

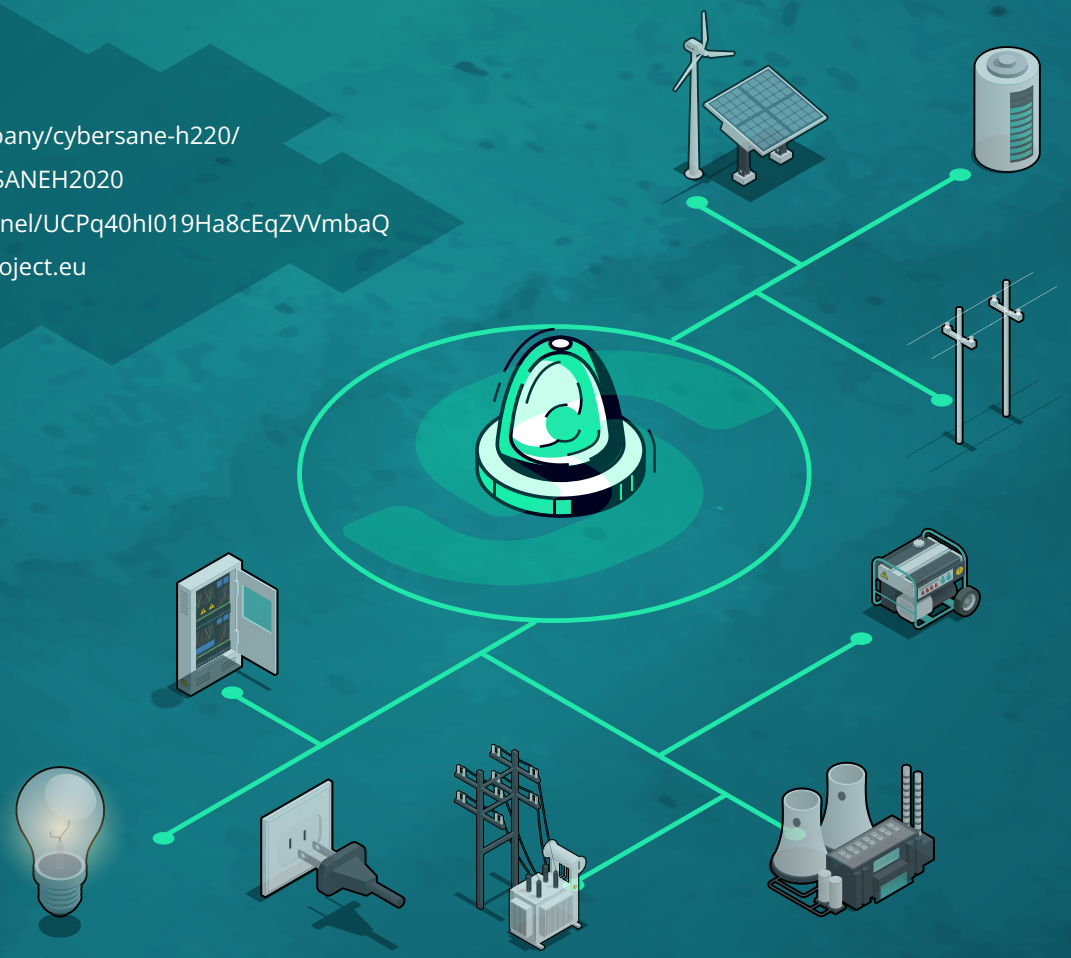
Sofia Spanoudaki, Chief Risk Officer

Prof. Vasiliki Danilatou, Director of STS Health Care Division

Konstantinos Kontakis, Software Engineer

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