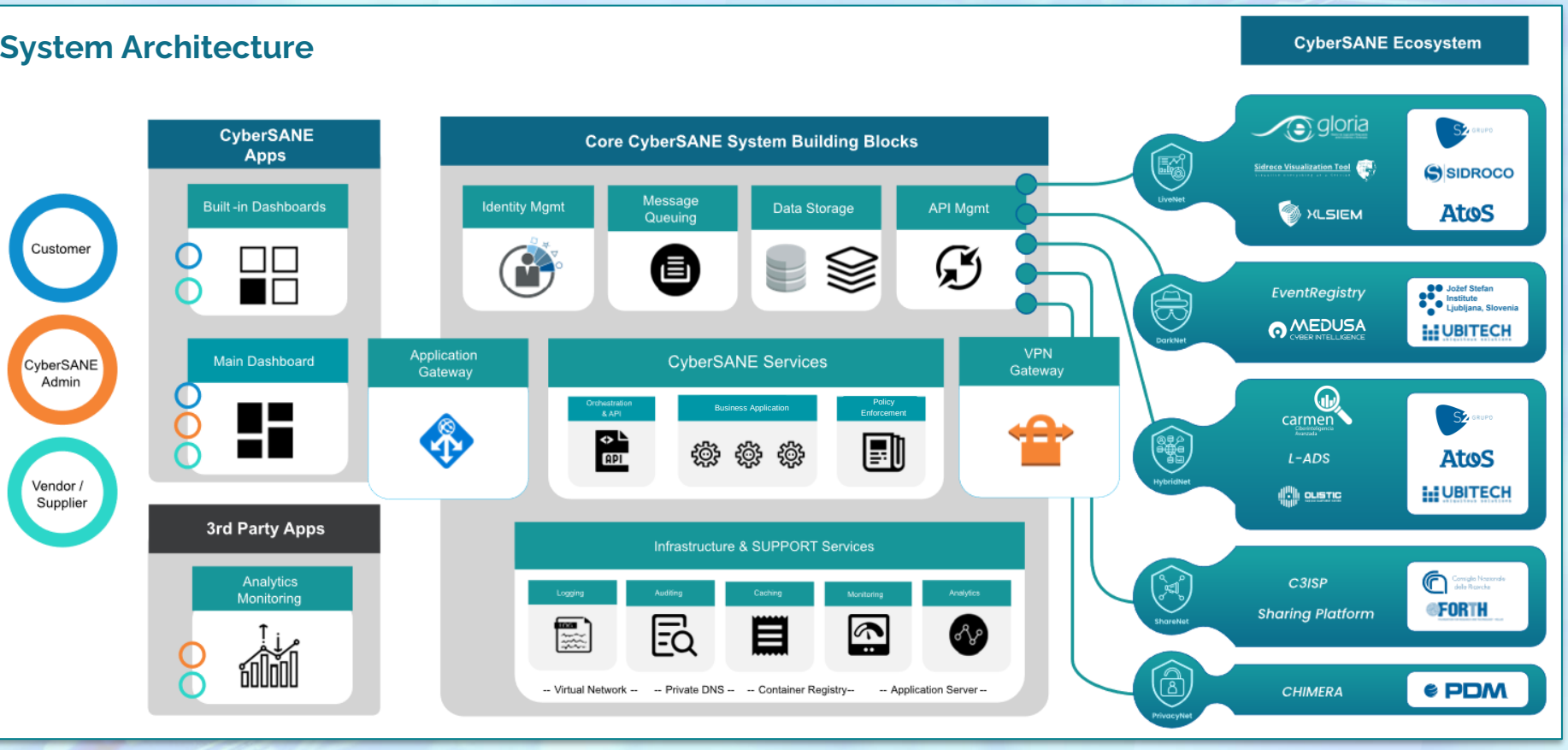
System Architecture



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

CYBERSANE

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

System Components: LiveNet

***LiveNet** is the Live Security Monitoring and Analysis interface platform component for preventing and detecting threats, and capable of mitigating the effects of an intrusion by monitoring, analysing and visualising internal live network traffic in real time.*

LiveNet features

Known Threat Detection

According to the conditions described in the attack patterns, security events are classified and evaluated against event correlation rules. If the patterns match, LiveNet provides an incident alert with contextualised information to be analysed as part of the incident management process.

Security Incident Detection

The incident management lifecycle provides contextualised information via alerts and messages once attack patterns are detected based on correlation rules. All security events attributes are analysed (payloads, attack vectors, criticality, etc).

Signature Generation

Considering the security analysts' investigation, the incident is documented along with any additional findings derived from the generation of attack signatures included in the incident knowledge base.

Attack Pattern Registration & Update

Registers new attack patterns, as part of the knowledge base to be prepared for the real-time detection of any security incident.

Live Monitoring

Real-time monitoring features for gathering, processing and classifying information from critical assets and devices. Relevant information is sent to a log centralisation system.

Security Event Identification & Classification

Retrieves and process information from the log centralisation system to extract, tag and classify relevant attributes.

LiveNet subcomponents

GLORIA can convert the incident-related data gathered from multiple sources into one unified and convenient format, cleaned to remove redundant and duplicate information.

SiVi is a human-interactive visual-based anomaly detection system that monitors and detects wormhole, selective forwarding, Sybil, hello flood and jamming attacks.

XL-SIEM can detect security incidents and integrate sensors from different vendors; it provides real time alerts, reporting and visualization capabilities.

LiveNet in CyberSANE Pilots

Solar Energy pilot: LiveNet detects the malware installation in a download of an unauthorized program.

Container Transportation pilot: LiveNet detects the malware installation, since it is monitored by means of the NIDS (Network Intrusion Detection System).

Healthcare pilot: LiveNet detects malware contacting known C2C-servers creates a security incident on the platform

***CyberSANE** is **a security incident handling, warning and response dynamic system** to **protect Critical Information Infrastructures (CIIs) against** different types of **cyberattacks and intrusions** based on knowledge and collaboration while allowing continuous learning during the whole lifecycle of an incident. CyberSANE is composed of five main components: LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet*

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

CYBERSANE

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

System Components: DarkNet

DarkNet *is the Deep and Dark Web Mining and Intelligence component which allows the exploitation and analysis of risks and threats by analysing textual and meta-data content from various electronic streams.*

DarkNet features

Incidents Identification

Searches the Dark Web and its sources of information, discussions and rumours about concrete cyber attacks, to properly analyse the global malware and cybersecurity activities.

Attack Techniques Identification

Based on the search results, it identifies attack techniques related to previous cyber-attacks, or new trends and techniques representing a threat.

Tools for Advanced Cyberattacks Identification

Identifies tools or traces of them related to previous cyber-attacks.

Cyber Actors Activity Reconstruction

Reconstructs the social graphs and user activities from specific forums to enable security experts to perform efficient investigations on various incidents

Textual & Meta-data Content Registration

Stores various data and metadata for further analysis and classification that can be useful for searching and identifying related cases and risks.

Risk & Threat Exploitation & Analysis

As an individual component, it is able to further analyse the harvested data to get the big picture of global malware cybersecurity activities including data aggregation, visualisation, etc.

DarkNet subcomponents

EventRegistry system is able to monitor and aggregate knowledge from mainstream and social media, including media articles and blog posts.

MEDUSA constitutes a sophisticated, modular, highly -configurable and -scalable web mining and intelligence platform that benefits from Artificial Intelligence and Big Data technologies to provide intelligence and real-time insights to non-IT domain experts, satisfying the multi-disciplinary needs of end-user organizations that require advanced web crawling, processing and analytics services. MEDUSA serves the DarkWeb Layer as a core component for crawling and curating texts from the dark web also feeding the ShareNet Layer to raise awareness about cyber incidents to end users.

DarkNet in CyberSANE Pilots

Solar Energy pilot: DarkNet checks the public IP against a database of known compromised IPs.

Container Transportation pilot: DarkNet searches related terms to look for information related to the attack.

Healthcare pilot: DarkNet gathers information about how to deal with the attack in the most effective way.

CyberSANE *is* ***a security incident handling, warning and response dynamic system*** *to* ***protect Critical Information Infrastructures (CIIs) against*** *different types of* ***cyberattacks and intrusions*** *based on knowledge and collaboration while allowing continuous learning during the whole lifecycle of an incident. CyberSANE is composed of five main components: LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet*

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

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

System Components: HybridNet

HybridNet *is the Data Fusion, Risk Evaluation and Event Management component which provides intelligence to perform effective and efficient analysis of security events coming from both information derived from other system components and on information and data produced by the incident to evaluate the security situation inside CIIs.*

HybridNet features

Anomalies & Incident Registration

Enables the creation and maintenance of the knowledge base of known anomalies and security incidents.

Anomalies Detection

Based on the analysis of the received data, identifies and evaluates security-related patterns associated with malicious or anomalous activities. It also allows also the identification of unusual activities matching the structural patterns of possible intrusions using Machine Learning techniques.

Attack & Behaviour Simulation

In parallel to the other features, provides a simulation tool enabling the testing of the impact of an attack on their system by modelling the attacks and threats paths and patterns, and allowing the reconstruction of valid chains of evidence associated with real security incidents already identified and registered on the system.

Decision Making Support

The data generated by HybridNet and other CyberSANE components is used to enable security professionals and experts to understand the impact of an attack in their systems, and to reach the proper decisions regarding the security aspects of their CIIs.

Alert & Notification Generation

Enables the generation and provision of near real-time notifications regarding real and/or potential vulnerabilities related to the assets of the CIIs.

HybridNet subcomponents

CARMEN is the Centre of Log Analysis and Mining of Events. It collects, processes and analyses information to generate intelligence mainly from the network traffic. It is made up of agents that compile traffic flows and help analysts to make decisions based on its results.

L-ADS (Live Anomaly Detection System) is a real-time network traffic monitoring and anomaly detection tool with novel Machine Learning capabilities which performs deep-packet inspection using its information for correlation of attacks in communications-based cyberthreats.

OLISTIC has a rich risk scenario library in a web-based software solution with a friendly and intuitive user interface. It can be easily configured by business process owners with significant time savings and reduced total cost of ownership over other solutions.

HybridNet in CyberSANE Pilots

Solar Energy pilot: HybridNet notifies the Security Expert about the detected anomaly and mitigation/investigation actions can be taken.

Container Transportation pilot: HybridNet detects access to the application is done from an unknown suspicious IP.

Healthcare pilot: HybridNet detects abnormal CPU- or RAM-consumption on the virtualized device

CyberSANE *is* ***a security incident handling, warning and response dynamic system*** *to* ***protect Critical Information Infrastructures (CIIs) against*** *different types of* ***cyberattacks and intrusions*** *based on knowledge and collaboration while allowing continuous learning during the whole lifecycle of an incident. CyberSANE is composed of five main components: LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet*

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

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

System Components: ShareNet

***ShareNet** is the Intelligence and Information Sharing and Dissemination component which provides necessary threat intelligence and information sharing capabilities within CIIs to enhance trustworthiness and identify incidents in a faster way.*

ShareNet features

Knowledge Sharing

Implements all required functionalities for sharing the data such as enforce attribute-based authorization, data enforce obligations, data manipulation operation, among others.

Attack Pattern Collection

Used as one of the main points for identifying new attack patterns from the internet, which can be properly registered in the CyberSANE platform through LiveNet component in order to allow real-time security incident detection.

Data Sharing Agreements

Allows the creation and maintenance of agreements between two or more entities, which can be either internal or external to CyberSANE, concerning the sharing of data or information to enable proper description and enforcement of all the mandatory rules, terms and conditions set for and agreed upon.

Protected Data Storage

Stores security incident data in a protected and secure way, ensuring its confidentiality and integrity at all implemented and supported CyberSANE scenarios.

ShareNet subcomponents

C3ISP

C3ISP defines a collaborative and confidential information sharing, analysis and protection framework as a service for cyber security management. Its innovation is the possibility to share information in a flexible and controllable manner inside a collaborative multi-domain environment to improve detection of cyber threats and response capabilities, still preserving the confidentiality of the shared information.

Sharing Platform

Sharing Platform provides cybersecurity related information exchange, integration with MeliCERTes CSP platform - a network for establishing confidence and trust among the national Computer Security Incident Response Teams (CSIRTs) of the EU Member States - and proposes cybersecurity solutions that allow ICT enabled organization and enterprises to focus on the products and services that they offer to citizens.

ShareNet in CyberSANE Pilots

Solar Energy pilot: ShareNet shares the information with the partners.

Container Transportation pilot: ShareNet shares the incident for avoiding the same attack in other infrastructures in the post incident activity section through a lesson learnt based on a Data Sharing Agreement.

Healthcare pilot: ShareNet notifies local CERT and other German hospitals on the threat to prevent damage at the other hospitals.

***CyberSANE** is **a security incident handling, warning and response dynamic system** to **protect Critical Information Infrastructures (CIIs) against** different types of **cyberattacks and intrusions** based on knowledge and collaboration while allowing continuous learning during the whole lifecycle of an incident. CyberSANE is composed of five main components: LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet*

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

CYBERSANE

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

System Components: PrivacyNet

PrivacyNet *is the Privacy and Data Protection Orchestrator component for the application and compliance of privacy mechanisms, confidentiality and data protection for sensitive incident-related information..*

PrivacyNet features

Personally Identifiable Information (PII) Detection

Detects personally identifiable data and information through a combination of predefined rules and Machine Learning models for matching typical PII patterns with fuzzy detection attempts.

Privacy Policy Enforcement

Policies refers to statements or documents disclosing some or all the methods a party gathers, uses, discloses and manages data. It provides the proper framework to support the declarative way required to define such usage and information owners, as well as semi-automatic conversion of said rules to a privacy engine, responsible for enforcing them.

Homomorphic Cryptography

Implements encryption schemes for allowing mathematical function to be executed directly on encrypted data, which will yield the same results as if the function was executed on plain text.

Format Preserving Attribute Based Encryption

Allows for the output format of encryption to be the same as the input format, using attribute-based encryption techniques to enable the encryption on partial data only.

Incident Data Redaction

Allows the removal of personal identifiable data in a security incident with data redaction techniques while keeping the redacted data useful for security experts.

PrivacyNet subcomponents

CHIMERA

CHIMERA is a dataflow application, integrated in a web user interface that can communicate with the Orchestration-Frameworks APIs allowing a user to manipulate knowledge and data generated by other tools. It can safeguard access to data through anonymization using a set of algorithmic techniques which make it very difficult to decode in a timely manner (less than a few million years). It prevents unintended access to sensitive data and ensure compliance with evolving data protection regulations, while facilitating data sharing between organizations.

PrivacyNet in CyberSANE Pilots

Solar Energy pilot: PrivacyNet provides the necessary anonymization .

Container Transportation pilot: PrivacyNet executes anonymization functions

Healthcare pilot: PrivacyNet anonymizes identifying information, i.e. assets IPs.

CyberSANE *is* ***a security incident handling, warning and response dynamic system*** *to* ***protect Critical Information Infrastructures (CIIs) against*** *different types of* ***cyberattacks and intrusions*** *based on knowledge and collaboration while allowing continuous learning during the whole lifecycle of an incident. CyberSANE is composed of five main components: LiveNet, DarkNet, HybridNet, ShareNet and PrivacyNet*

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