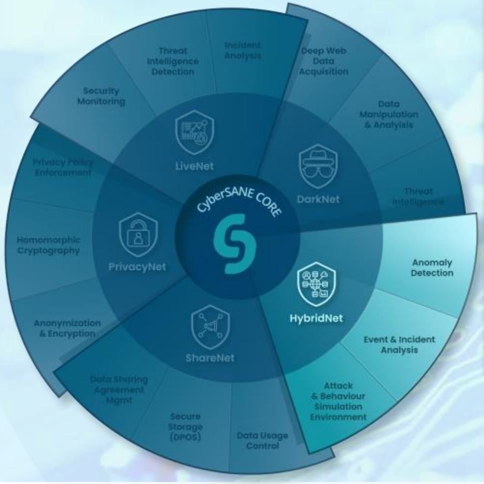
CYBERSANE

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.*



CyberSANE CORE
LiveNet
DarkNet
HybridNet
ShareNet
PrivacyNet
Threat Intelligence Detection
Incident Analysis
Deep Web Data Acquisition
Data Manipulation & Analysis
Threat Intelligence
Anomaly Detection
Event & Incident Analysis
Attack & Behaviour Simulation Environment
Data Usage Control
Secure Storage (DPOS)
Data Sharing Agreement Mgmt
Anonymization & Encryption
Homomorphic Cryptography
Privacy Policy Enforcement
Security Monitoring

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.