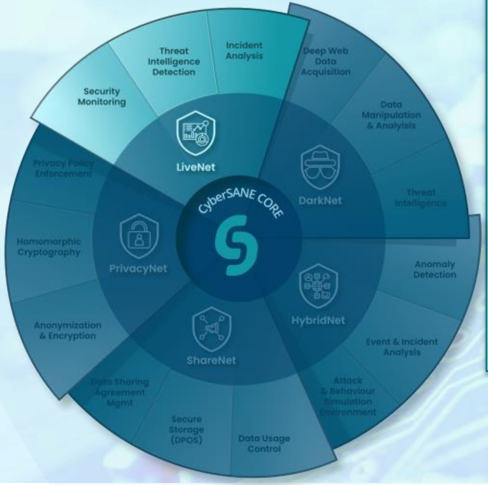
CYBERSANE

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.


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

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.