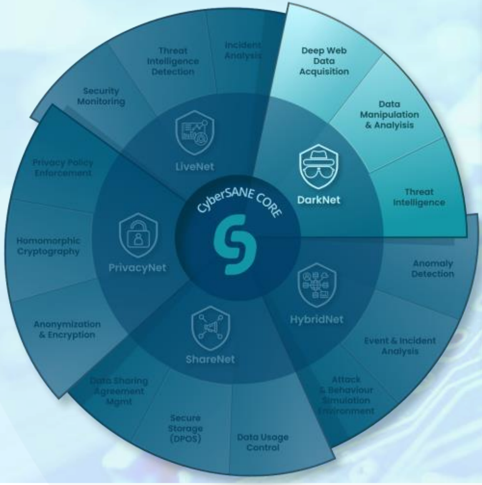
CYBERSANE

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.*



CyberSANE CORE
LiveNet
DarkNet
HybridNet
ShareNet
PrivacyNet
Deep Web Data Acquisition
Data Manipulation & Analyisis
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
Threat Intelligence Detection
Incident Analysis

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

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

MEDUSA CYBER INTELLIGENCE

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.