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.