EU-funded project CyberSANE to transform security incident detection and handling systems

The 36-month project with funding of € 4.985.550 focuses on the development of cybersecurity solutions in the form of reliable, flexible, scalable, and efficient ICT components for Critical Infrastructures Information (CIIs).

TRANSPORT AND MOBILITY | SECURITY | HEALTH

CyberSANE project has been funded by the European Commission as part of its H2020 Programme under the call SU-ICT-01-2019 and topic “Dynamic countering of Cyber-attacks”. The project foresees the development of a system addressing both technical and cognitive challenges related to the identification, prevention, and protection against attacks on critical infrastructures through collecting, compiling, processing and fusing of all individual incident-related information for ensuring the integrity and validity of Infrastructures, helping decision-makers to understand the technical aspects of an attack and draw conclusions on how to respond.

According to a Ponemon Institute study, critical infrastructure providers have been overloaded by cyberattacks in the past two years, and 90% of them have been victims of cyberattacks since 2017, with half of the attacks resulting in downtime of operations. The survey included respondents from different regions and sectors such as utilities, energy, health, and transport, which store highly sensitive information and are responsible for essential services.

CyberSANE will design an advanced, configurable and adaptable, security and privacy incident handling system with the aim to improve, intensify and coordinate the overall security efforts for the effective and efficient identification of threats, and the investigation, mitigation, and reporting of multi-dimensional attacks within the interconnected web of cyber assets involved in critical infrastructure information and security events. For this purpose, the CyberSANE system includes a series of tools and components:
- LiveNet (Live Security Monitoring and Analysis): Capable of preventing and detecting threats, and in case of a declared attack, capable of mitigating its infection/intrusion effects.
- DarkNet (Deep and Dark Web Mining and Intelligence): Allows the analyses of security, risks and threats related information embedded in User Generated Content (UGC) via the dark web and similar sources.
- HybridNet (Data Fusion, Risk Evaluation, and Event Management): Provides the intelligence required to perform effective and efficient analysis of a security event based on information collected by the LiveNet and DarkNet components.
- ShareNet (Intelligence and Information Sharing and Dissemination): Provides threat intelligence and information with sharing capabilities within CIIs and other involved parties to determine the trustworthiness of information sources as soon as the data is received.
- PrivacyNet (Privacy & Data Protection Orchestrator): Manages and orchestrates the application of innovative privacy mechanisms. It also maximises achievable levels of confidentiality and data protection towards compliance with GDPR directives in the context of protecting sensitive incident-related information within and outside CIIs.

In order to validate the benefits and features of the CyberSANE system, three pilots covering different sectors identified as critical to security and EU financial impact will be executed: solar energy production, storage, and distribution service operated by Lightsource Labs in Ireland; a container cargo transportation service managed by the Port of Valencia in Spain; and a real-time patient monitoring and treatment service provided by Klinikum Nuremberg in Germany.

The project is coordinated by PDMFC (Portugal) and involves 15 partners with different areas of expertise to address all the development of the CyberSANE System and the proper validation of the scenarios: Atos (Spain), CNR (Italy), S2 Grupo (Spain), INRIA (France), Maggioli (Italy), Ubitech (Cyprus), JSI (Slovenia), FORTH (Greece), Sphynx Technology (Switzerland), KU Leuven (Belgium), Sidroco Holdings (Cyprus), University of Brighton (UK), ValenciaPort (Spain), Lightsource Labs (Ireland), and Klinikum Nuremberg (Germany).

For more information please visit: http://www.cybersane-project.eu/
Follow CyberSANE project on Twitter and LinkedIn

Beitragender

Bereitgestellt durch

CyberSANE

Spain

Website

Verwandte Projekte

HORIZON 2020

PROJEKT

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

CyberSANE

11 Dezember 2023

Letzte Aktualisierung: 14 Februar 2020

Permalink: https://cordis.europa.eu/article/id/413492-eu-funded-project-cybersane-to-transform-security-incident-detection-and-handling-systems/de