CyberSANE Pilot Scenarios

Solar Energy

CyberSANE will protect the Smartly Integrated Distributed Energy platform (SIDE) of an energy supplier which produces, store and distributes solar energy. It will provide its SIDE and components with robustness against threats to the back-end via unauthenticated remote access to IoT components as well as other entities which may change data, disrupt services or IT/communication systems processing and transmitting sensitive data.

Transportation of Container Cargo

The transportation of container cargo services requires protection of IT and port community systems. This pilot will be carried out at the sixth largest port in Europe in terms of traffic volume. CyberSANE will provide security for complex threat scenarios which may disrupt port operations, facilitate illegal activities, unauthorised access to corporate networks, and interference with authorisation processes for vessels.

Health Records

CyberSANE will provide the clinic with monitoring and protection of real-time patient Electronic Health Records (EHR) and Electronic Medical Records (EMR), against ransomware attacks and attacks on vulnerable medical services which may destroy or alter critical information (ultimately resulting in physical injury to patients).

For more information visit www.cybersane-project.eu

Follow us on @CyberSANEH2020 CyberSANE

Contact

luis.campos@pdmfc.com

@CyberSANEH2020

CyberSANE

CyberSANE-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 833683

CYBERSANE

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

www.cybersane-project.eu

CyberSANE

Over the past decade, various industries have required optimisation of operations with a high degree of flexibility, scalability and efficiency. Industry has also needed efficient communication, coordination of advanced services and processes which has led to the rise of Critical Information Infrastructures (CIIs) such as those related to health care, energy and transportation, which rely on robust and reliable ICT components and complex ICT infrastructures which integrate multiple novel technologies for operation optimisation.

The amount of information (including characteristics) and data used, gathered and shared has made CIIs vulnerable to threats or attacks from hackers and cyber criminals. These hackers and cyber criminals are constantly evolving due to the technical capabilities and resources available to them from various sources including the Dark and Deep Web.

To tackle these threats as well as protect the CIIs against cybercrime, CyberSANE will implement an innovative and novel approach. CyberSANE will develop a dynamic security incident handling, warning and response system to help European CIIs.

The CyberSANE solution is compliant with the applicable legal and regulatory framework and builds on knowledge and collaboration among CIIs to allow continuous learning during the whole lifecycle of an incident(s).

Important Cyber-attacks to CIIs

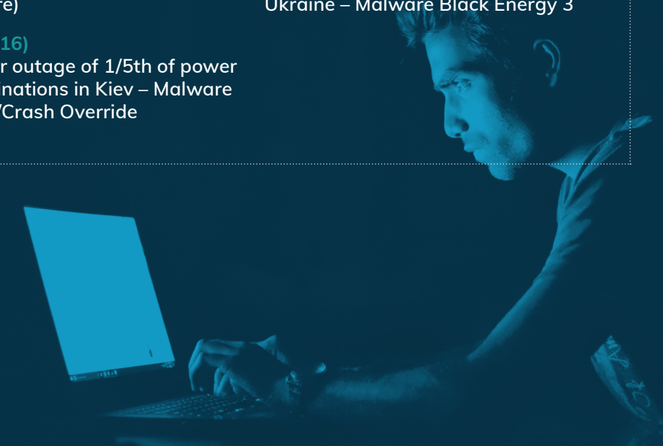
Norway (2018)
Healthcare data of more than half of the country's population stolen

Ukraine (2017)
Infection of NotPetya of radiation monitoring system at Chernobyl nuclear power plant forcing manual control – Malware infection (ransomware)

Ukraine (2016)
1hour power outage of 1/5th of power supply destinations in Kiev – Malware Industroyer/Crash Override

Israel (2016)
2-day shutdown of part of the computer system dealing with cyberattacks of the Israeli Electricity Authority - Malware infection by phising attack

Ukraine (2015)
Few hours power outage in western Ukraine – Malware Black Energy 3



CyberSANE Components

LiveNet
Live Security Monitoring and Analysis interface platform component for preventing and detecting threats. It is also capable of mitigating the effects of an intrusion by monitoring, analysing, and visualising internal live networks traffic in real time.

DarkNet
Deep and Dark Web mining and intelligence. It will allow the exploitation and analysis of risks and threats by analysing textual as well as meta-data content from various electronic streams.

HybridNet
Data fusion, risk evaluation and event management will provide intelligence to perform effective and efficient analysis of security events. This will come from both information derived from other system components, as well as from information and data produced by the incident to evaluate the security situation inside CIIs.

ShareNet
Intelligence, information sharing and dissemination providing necessary threat intelligence and information sharing capabilities within CIIs. This will enhance trustworthiness and identify incidents in a more efficient manner.

PrivacyNet
Privacy and data protection orchestrator for the application and compliance of privacy mechanisms, confidentiality and data protection for sensitive incident-related information.