System Components: PrivacyNet

PrivacyNet is the Privacy and Data Protection Orchestrator component for the application and compliance of privacy mechanisms, confidentiality and data protection for sensitive incident-related information..

PrivacyNet features

Personally Identifiable Information (PII) Detection

Detects personally identifiable data and information through a combination of predefined rules and Machine Learning models for matching typical PII patterns with fuzzy detection attempts.

Privacy Policy Enforcement

Policies refers to statements or documents disclosing some or all the methods a party gathers, uses, discloses and manages data. It provides the proper framework to support the declarative way required to define such usage and information owners, as well as semi-automatic conversion of said rules to a privacy engine, responsible for enforcing them.

Homomorphic Cryptography

Implements encryption schemes for allowing mathematical function to be executed directly on encrypted data, which will yield the same results as if the function was executed on plain text.

Format Preserving Attribute Based Encryption

Allows for the output format of encryption to be the same as the input format, using attribute-based encryption techniques to enable the encryption on partial data only.

Incident Data Redaction

Allows the removal of personal identifiable data in a security incident with data redaction techniques while keeping the redacted data useful for security experts.

PrivacyNet subcomponents

CHIMERA

CHIMERA is a dataflow application, integrated in a web user interface that can communicate with the Orchestration-Frameworks APIs allowing a user to manipulate knowledge and data generated by other tools. It can safeguard access to data through anonymization using a set of algorithmic techniques which make it very difficult to decode in a timely manner (less than a few million years). It prevents unintended access to sensitive data and ensure compliance with evolving data protection regulations, while facilitating data sharing between organizations.

PrivacyNet in CyberSANE Pilots

Solar Energy pilot: PrivacyNet provides the necessary anonymization .

Container Transportation pilot: PrivacyNet executes anonymization functions

Healthcare pilot: PrivacyNet anonymizes identifying information, i.e. assets IPs.

*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*