Fraunhofer IOSB

FRAUNHOFER INSTITUTE OF OPTRONICS, SYSTEM TECHNOLOGIES AND IMAGE EXPLOITATION

PREEMPTIVE: PREventivE Methodology and Tools to protect utilitIEs

Steffen Pfrang, Jörg Kippe, the PREEMPTIVE consortium

The PREEMPTIVE project seeks to prevent and detect cyber-attacks against utilities by developing innovative methods and tools in security risk assessments and intrusion detection.

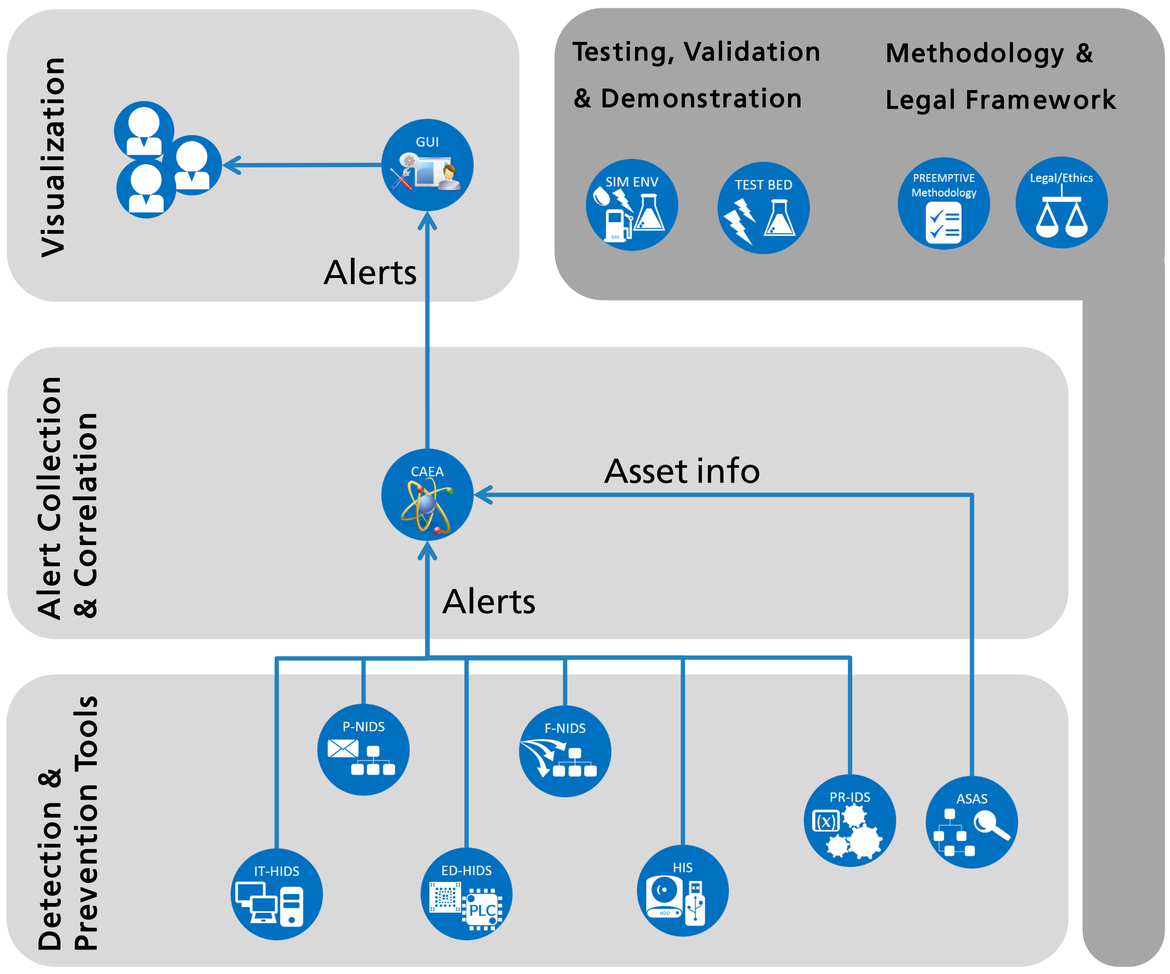
Project Objectives → Main Outcomes

- Taxonomy: Classification of utility networks and cyber threats → **Report**
- Modelling: Virtual environments for simulation purposes including gathering data on cyber attacks → **Software**
- Software detection (network, host and process based) and event correlation tools → **Software**
- Cyber Defense Methodology Framework → **Guidelines**
- Ethics, Social Impact → **Report**

Selected Results

- Payload-based network intrusion detection system (NIDS)
- Flow-based NIDS
- Host-based intrusion detection system (HIDS) for IT components used in industrial control systems (ICS)
- HIDS for embedded devices (e.g. PLCs)
- Integrity of storage devices (e.g. USB flash drives)
- Process-based intrusion detection system
- Asset Assessment: Asset detection and vulnerability testing for ICS and field devices

Project Architecture



The PREEMPTIVE detection architecture is based on alerts from

- host and network intrusion detection systems,
- on alerts generated from the process observation
- as well as on asset and vulnerability information gathered from passive network sniffing up to active probing.

A correlator generates an overview of security status which is presented to the operators.

www.preemptive.eu

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 607093.