SAFECARE NEWSLETTER SEPTEMBER 2019

News

Awareness Event in Leuven - SAFECARE will be holding its first awareness event in Leuven, in September.
Bucharest Focus Group - BEIA Consult hosted the SAFECARE partners in Bucharest for the third focus group meeting.

Work Package Progress

WP1

D1.1 : H –Requirement No 2 -
Consent templates

- Delivered 19/11/2018

D1.4 : POPD –Requirement No 9 –
Nomination of DPOs

- Delivered 26/09/2018

D 1.2 : POPD –Requirement No 2 – Declaration of compliance with national law

- Delivered 25/09/2018

D 1.3 : GEN –Requirement No7 – Annual ethic report

- In review before delivering end of August

WP2

T 2.1 Technical and scientific coordination

- with Work Package Leaders
- Preparation of annual progress report D2.1 M12

T2.2 Administrative and financial tasks

- Templates for biannual financial report
- Upload of first report on cumulative expenditures

T2.3 Quality documents and deliverables management

- Quality plan by EOS
- Designation of reviewers for all deliverables

WP3

T3.2. State-of-the-art analysis and known vulnerabilities (M3-M12)

- A first draft of D2.2, that includes a list of physical and cyber vulnerabilities, how they might impact the likelihood of attacks and their effects, and the state-of-the-art analysis about security controls in health infrastructures, was delivered in M6.

T3.3. Requirements analysis (M1-M12)

- Initial requirements analysis in terms of physical security solutions, cyber security solutions, crisis management, communication and coordination strategies (D3.4) was delivered on M6.
- Lexicon about crisis management applicable to cyber security and physical security was also delivered in M6 as an annex of D3.4.

T3.4. Definition of the cyber-physical scenarios of threat (M3-M9)

- Identification and formalization of the relevant use-cases and complex attack scenarios against critical health infrastructures. The resulting report (D3.6) was delivered in M9.

T3.5. Cyber-physical risk assessment and impact analysis (M9-M35)

- Kick-off of the task..

T3.6. Ethics, data privacy, data confidentiality, European and national regulations (M1-M36)

- Analysis of ethical, privacy and confidentiality constraints. The resulting report (D3.9) was delivered in M6.

WP4

T4.1 –Suspicious behaviour system (Started in February 2019):

- Requirements capture complete and definition of solution nearing completion
- Research on current video provision in use case sites progressing
- Definition of test bed hardware demonstrator for video underway

T4.2 – Intrusion and fire detection system (Started in February 2019):

- Requirements capture complete and definition of solutions nearing completion
- Access control management system at ASLTO5 and AP-HM has been determined
- Definition of test bed hardware demonstrator for access control underway

T4.3 – Data collection system from ICS, SCADA… (Started May 2019):

- Requirements capture and solution definition underway
- Research on fire mgt. sensors at hospitals has been determined, and others underway
- Definition of test bed hardware demonstrator for sensors underway

T4.4 – Mobile service for integrated alerting system (Started Feb 2019):

- Requirements collection complete and definition of system architecture underway
- First mockups of Safecareapp produced
- Proposal of data exchange format (JSON and EDXL)

T4.5 – Building monitoring system (Started in April 2019):

Alignment of planned functionality with global architecture and mobile service underway

WP5

T5.1 - IT threat detection system (Started in May 2019):

- The solution for network intrusion detection system has been defined

- Architecture with the AI module (machine learning algorithms) has been defined and reviewed
- Analysis of some supervised and unsupervised algorithms

T5.2 - BMS threat detection system (Started in May 2019):

- Devised general hospital network architecture (to be validated with questionnaire)
- Analysis of the main protocols to be supported in the BMS sensor for monitoring hospital networks
- PoCdeployment at Moncalieri hospital for knowledge acquisition

T5.3 - Advanced file analysis system (Started in May 2019):

- Development of a connector with D5.2 so that D5.2 automatically submits extracted files for analysis
- DICOM images with fictive (patient/physician) metadata have been generated: DICOM sample files, viewer application and relevant references
- Test phase of the developed connector regarding performance
- Specification of the advanced file analysis system (D5.5)

T5.4 - E-health devices security analytics (Started in February 2019):

- Acquisition of data sources that contains logs from Philips radiology equipment
- General exploration of logs to learn the type of information logged and the relation between different log tables
- Architectural work on log retrieval and security analytics infrastructure
- Collection of past cyber security events concerning Philips devices
- Perform analytics on different types of log files (Event logs, SSH logs, Whitelisting and antivirus logs, Configuration logs)
- Examples of use cases under consideration: Software whitelisting / antivirus engine status, Detecting and analyzing cases of unauthorized access, Use of device security features (e.g. auto versus manual logon)

T5.5 -Cyber threat monitoring system (Started in May 2019):

- The solution for cyber threat monitoring system has been defined

- Decision to self-supervise the SAFECARE solution with the cyber threat monitoring system

WP6

T6.1 Specification of the global architecture (M9-M16)

- The global architecture schema has been defined. It reports all the interconnections and message flows among SAFECARE modules
- Relevant terms have been defined:
- Security events, are detected by cyber or physical security modules and are automatically evaluated in order to understand if they can be considered as alerts
- Alerts, are shown to human operators (e.g. SOC) that can check if they are true alerts or false positives
- Incidents, are human-verified alerts that are sent to decisional modules (WP6) to be stored and elaborated

T6.2 Data exchange layer (M6-M24)

- MQTT has been chosen as the protocol to implement publish-subscribe mechanism
- The data exchange layer is the only one module that can directly interact with the central database

T6.3 Central database (M6-M24)

- Main elements that will be stored in the central database have been defined

T6.4 Impact propagation model and decision support model (M6-M25)

- Requirements and functionalities of this module have been generally defined as well as its internal architecture

T6.6 Hospital Availability Management System (HAMS) (M9-M25)

- Functionalities of the HAMS have been defined
- EDXL-HAVE standard has been studied and analysed

- A first draft of the user interface has already commented by ASLTO5

WP8

T8.1 - Dissemination and Communication Strategy

- Strategy delivered M3
- Promotion material created and disseminated at events. Copies available online for partners to print their own.
- Material being translated into multiple languages (French and Italian initially)

T8.2 – Dissemination and communication, implementation and project events

- Work is active and ongoing on the task through the three main communications channels: Website, Twitter and LinkedIn.
- Event promotion has started for Leuven –agenda and promotional material has been created.

Upcoming Events

SAFECARE Awareness Event, Leuven - September 18 2019
Mediterranean Security Event, Crete - 29-31 October 2019 (PDF, 0.4MB) - More Informatio