CUREX

CUREX Newsletter

Issue 02 | April 2020

WELCOME TO THE SECOND CUREX NEWSLETTER!

TABLE OF CONTENTS

We are pleased to announce the publication of the second issue of the CUREX newsletter. If you are interested in cybersecurity and privacy in healthcare, you are at the right place!

CUREX is a 3-year Research and Innovation Action (RIA) from 2018 to 2021 funded under Horizon 2020 focusing on producing a novel, flexible and scalable situational awareness-oriented platform, addressing comprehensively the protection of the confidentiality and integrity of health data. CUREX kicked-off in Piraeus, Greece on 24-25 January 2019.

The vision of CUREX is to safeguard patient privacy and increase their trust in the currently vulnerable critical healthcare information infrastructures, especially in cases where data is exchanged among healthcare stakeholders within any business, operational and systemic cross-border environment. By leveraging novel methods on ontological health data modelling, vulnerability discovery, threat intelligence, cybersecurity, and privacy risk assessment methodologies, and state-of-the art in blockchain technologies for health data, CUREX aims at enabling secure and authorized sensitive health data exchange.

PROJECT INFORMATION

CUREX: seCURe and pRivate hEalth data eXchange
GRANT AGREEMENT ID: 826404
START DATE: December 1st, 2018
END DATE: November 30th, 2021
COORDINATOR:
University of Piraeus Research Center

STAY TUNED!

Stay updated on all our latest news, developments, research and general information regarding the CUREX project.
Stay tuned @ www.curex-project.eu!

@CUREX_H2020

curexproject

CUREXH2020

SUBSCRIBE here to our newsletter!

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404

OVERALL CUREX ARCHITECTURE DESIGN

The CUREX solution will analyse information coming from the monitoring infrastructure to compute cybersecurity and privacy risk scores associated to the data exchange in a Health domain. CUREX has five discrete areas: (i) Asset and Vulnerability Discovery, whose goal is to discover the system's assets and any information related to their associated vulnerabilities; (ii) Threat Intelligence, aiming at detecting real time abnormal behaviours on users, and devices, as well as anomalies in the data in order to identify new and unknown threats; (iii) Risk Management, aiming at producing risk scores and optimal safeguards towards a cyber strategy of the healthcare organisation; (iv) Trust Enhancing, which will make use of decentralized platform based on blockchain technology to store and share private and sensitive data; and (v) Application and Visualisation, to display the platform dashboard in a synthetized way as depicted in the figure.

EACH AREA INCLUDES ONE OR MORE OF THE FOLLOWING TOOLS:

- **Asset Discovery Tool (ADT)**
- **Knowledge Extraction and Analytics (KEA)**
- **Vulnerability Discovery Manager (VDM)**
- **Threat Intelligence Engine (TIE)**
- **Cybersecurity Assessment Tool (CAT)**
- **Privacy Assessment Tool (PAT)**
- **Optimal Safeguards Tool (OST)**
- **Private Blockchain (PrB)**
- **Health professional Application (HPA)**
- **Patient Application (PA)**
- **CUREX Visualization Tool (CVT)**

The general workflow of the information within the CUREX toolkit is as follows:

(i) Assets are discovered by the ADT and the information associated to the services, OS, dependencies, and/or any other valuable information to be used for the risk assessment process;

(ii) Discovered assets are sent to the VDM tool in order to search for vulnerabilities;

(iii) The list of vulnerabilities associated to the assets from the monitored infrastructure is shared with the TIE and KEA for further analysis. Events are processed and correlated, and the outcome of this module is then shared with the risk assessment toolkit;

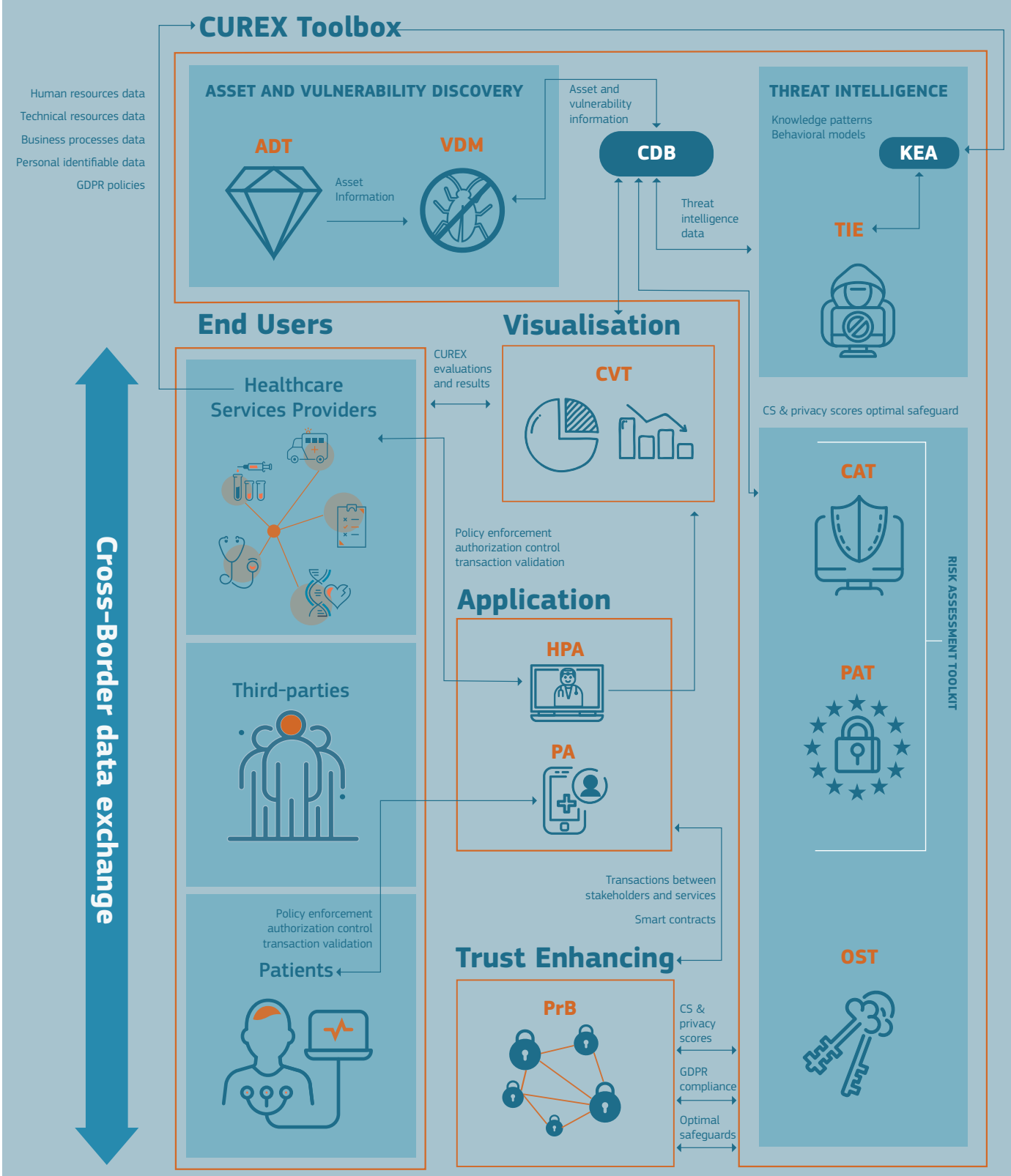
(iv) CAT and PAT performs the cybersecurity and privacy risk assessment respectively for the events selected by the TIE;

(v) OST is a risk control and decision support tool that proposes optimal safeguards to be executed based on the risk levels computed by the risk management toolkit components as well as cost-benefit analysis of cyber controls.

(vi) the cybersecurity and privacy risk assessment scores and some metadata information, as well as description of the optimal cyber strategy proposed (i.e., optimal security measures) will be stored in the PrB. This latter will deal with the transactions between stakeholders and services of the CUREX platform and will be in charge of generating smart contracts to the PA and HPA.

(vii) Finally, end-users can perform actions such as policy enforcements, authorisation controls, and transaction validations through their respective applications.

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404



This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404

ASSET DISCOVERY TOOL OF CUREX ARCHITECTURE

The first step in the CUREX pipeline is to have a complete imprint of all the assets available in the institutions that are going to perform a data exchange so that they can be later analysed in search of possible vulnerabilities or privacy breaches.

Therefore, the Asset Discovery Tool (ADT) is thought to discover all the devices that are connected to the hospital's network and as much information as possible from them. More specifically, it discovers (when it is possible) their IP and MAC addresses, their operating systems, and their open ports. Moreover, it tries to discover what service (or software) is listening at each port and their versions.

In order for this being possible, the tool has been conceived as a distributed application, in which an agent is running in each isolated network. When an agent discovers information about the devices in the network, it sends this information to a central node which stores all the information. Any other application that desires to make use of the information must retrieve it from this central node making use of a security token that must be provided by the tool administrator.

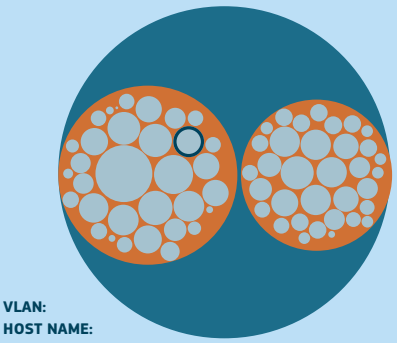
In the central node, the information is stored in two different ways: i) in a relational database; and ii) using a semantic representation by means of an ontology.

The semantic representation allows other tools have a meaningful sight of the assets that are available in the current ecosystem.

Moreover, this central node incorporates a Natural Language Processing (NLP) module that allows the network administrator to send the information of a given network in natural language. This module can be useful in the cases in which the agent cannot be run in a network for any reason, but the administrator has some information about its devices and/or services.

As a securization effort, the central node can be used with a Trusted Platform Module (TPM) which checks that the hardware of the device hosting the node has not been altered from its set up. In the case that a change is detected, all the security tokens are disabled until the tool administrator checks the change and, if it was a legitimate change, he/she can enable all the tokens again.

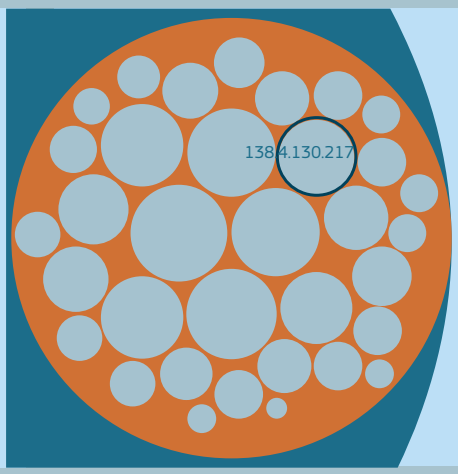
Finally, the tool incorporates a visualization module that allows the administrator to have a global perspective of the system with just a glance. This module also allows the administrator to focus on a specific network or, even, on the information about a specific device.



VLAN:
HOST NAME:
OPERATING SYATEM:

Port	Service	Status

Visualization of the VLANs that have been already scanned



VLAN: beast_vlan1
HOST NAME: 138.4.130.217
OPERATING SYATEM: Microsoft Windows Server 2008 R2 or Windows 8.1

Port	Service	Status
135	Microsoft Windows RPC	open
139	Microsoft Windowsn netbios-snn	open
445	Microsoft Windowsn 7-10 Microsoft-ds3580	open
3389	Microsoft Terminal Service	open
3580	Mbedthis-Appweb	open
5938		open
6002	Safenet Sentinel Protection Server	open
7001		open

Visualization of a specific VLAN and the information about one of its devices.

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404

KNOWLEDGE EXTRACTION & ANALYTICS (KEA) COMPONENT OF THE CUREX PLATFORM

Nowadays, the modern health infrastructures are threatened by intrusions and real-time attacks related to privacy and cyber-security. Therefore, there is a demanding need for proposing novel methodologies to predict future attack incidents based on detection of early warnings and identify new threat patterns.

Knowledge Extraction Analytics (KEA) is a component of the CUREX platform, identifying a set of effective techniques that harvest the knowledge that is extracted from health data sources or network monitoring, in order to reveal vulnerabilities and the profile of threats that appear and happen in health systems.

The main functionalities of KEA component, the reference architectures and the constituent analytics techniques have been presented and a detailed analysis of the architecture has been implemented, aiming to reveal all the interconnections between KEA and the other CUREX platform components, such as the Threat Intelligence Engine (TIE) component that will eventually encompass KEA.

Specific methods for detecting threats, identifying threat patterns and predicting possible threats tailored to the CUREX setting have been designed and implemented. This task plays a key role in the CUREX platform architecture, as it comprises complementary techniques for vulnerability analysis in the Vulnerability Discovery Manager component, through providing threat patterns. Moreover, the analytics performed in the context of KEA will be complemented by the work to be performed in TIE. Finally, KEA receives input from both the Asset Discovery Tool and TIE.

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404

CUREX BLOCKCHAIN DESIGN SPECIFICATIONS

A comprehensive documentation including all necessary information on the operational design specifications of the CUREX's Private Blockchain has been created. The technology selection and rationale behind the CUREX's Private Blockchain design were introduced.

In this regard, a comprehensive study of the state-of-the-art about permissioned ledgers was presented by surveying current solutions and approaches consolidating work from the blockchain requirements elicitation done within the use cases analysis & requirements. Moreover, an evaluation considering the execution environment and capabilities of smart-contracts have been taken as an input to that end.

As a result, a blockchain architecture proposal that reflects the flexibility to be integrated not only with the rest of the components of the CUREX platform but also with other permissioned ledgers is presented. The modularity achieved by the proposal also offers advantages for the Private Blockchain to adapt and evolve with time to different circumstances such as an increase on the platform users and scenarios where partial distrust may be present. Furthermore, the proposed implementation allows an easy way to define and manage different assets through smart-contracts that can be updated (as chain codes in Hyperledger Fabric can be updated) which contributes to the maintainability of the code.

The material in this document has served as the main input for the Blockchain release, guiding the blockchain implementation and smart-contracts development.

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404

MARKET ANALYSIS OF THE CUREX SOLUTION

As part of the CUREX project, a report was compiled analysing the market for the proposed solution, in order to document the strategies leading towards market adoption. This report was conducted under the auspices of WP2 in regard to the "Requirements, system Design & use cases".
The 5 Forces of Porter analysis indicates that the market is quite competitive, but the industry is attractive with sustainable growth opportunities. The bargaining power of suppliers is considered low due to the significant number of competitors offering similar services. The bargaining power of buyers is considered to be medium. On the one hand, several existing Cyber Security (CS) solutions provide a level of service; on the other hand, CUREX includes a bundle of unique tools that no other CS solution offers currently in the market.

The threat of new entry is assessed as medium. Although the barriers of entry to create a product like CUREX are high, the market itself is quite lucrative, and hyperscalers are greatly incentivised to invest. The threat of substitute products is considered low-medium since there are already products offering similar services with some of CUREX services. Still, none of those products can provide the bundle of tools CUREX does. Industry Rivalry is considered to be medium for the same reason; however, this might change once CUREX is launched, opening a new market in the CS sector.

Following that, our PESTLE analysis indicated that CUREX would be adopted in the European Market as well as Globally, especially in terms of key partners being utilised to launch the product. The EU market as a whole and the market CUREX is going to address to in the EU can be assessed as favourable for initiating CUREX from all aspects; Political, Economic, Social, Technological, Legal and Environmental.

A significant result also came through our ERRC (Eliminate-Reduce-Raise-Create) grid analysis, indicating that CUREX is eligible for creating a new market (blue ocean market environment). By creating a new market, CUREX would be the first to enter with literally little to no competition enjoying all the advantages of an early launch and deployment. Moreover, CUREX would already have an established customer base due to the participation of key end-user partners in the CUREX consortium and would be able to promote itself through those partners.

Finally, on our SWOT analysis, we have assessed the Strengths, the Weaknesses of the internal environment of CUREX and external opportunities and threats; thus, determining the strategic advantage of CUREX as quite high.

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404

CUREX EVENTS

CUREX at European and International events – the highlights

6th annual EAB.Cyber Meeting

The 6th annual EAB.Cyber Meeting, organized by the European Security and Defence College (ESDC), the entity within the EU that provides training and education at European level, in the field of the Union's Common Security and Defence Policy (CSDP) took place in Brussels, Belgium on November 19, 2019. CUREX project's objectives and innovations were presented to the audience comprised of representatives from academia, industry, national authorities and the military.

Read more

Safer Internet Day (SID) 2020

On February 11, 2020, Cyprus celebrated the Safer Internet Day 2020 with a major event in Nicosia, which was dedicated to encouraging everyone to play their part in creating a better Internet. As the main keynote speaker, Project Coordinator Prof. Christos Xenakis tried to inspire a safer and more efficient use of the Internet by informing students and their teachers about the threats that currently all digital infrastructures face. He had also the opportunity to talk about CUREX as a solution which aspires to safeguard the healthcare domain against the threats that are affecting it.

Read more

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404

21st InfoCom World Conference

The 21st InfoCom World Conference, the annual meeting place for digital industry executives, as well as all who use specialized tools and services in order to realize Digital Transformation, took place in Athens, Greece on November 26, 2019. CUREX project's solutions and use cases were presented in a parallel session titled as "5G Science Meeting" at the special sub-session over "Security Challenges in Modern 5G Environments".

Read more

Critical Infrastructure Security and Resilience (CISaR) workshop

The Critical Infrastructure Security and Resilience (CISaR) workshop took place in Gjovik, Norway, on January 30-31, 2020. The workshop was organized by the Critical Infrastructure Security and Resilience Research Group of NTNU and brought together research teams across Europe collaborating in R&D projects, hoping to create a forum for exchanging ideas and forming new synergies. CUREX was introduced to the audience as a comprehensive solution to secure digital healthcare infrastructures, which are nowadays recognized globally as Critical Information Infrastructures.

Read more

Discover more events where CUREX was present at curex-project.eu/content/newsevents

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404

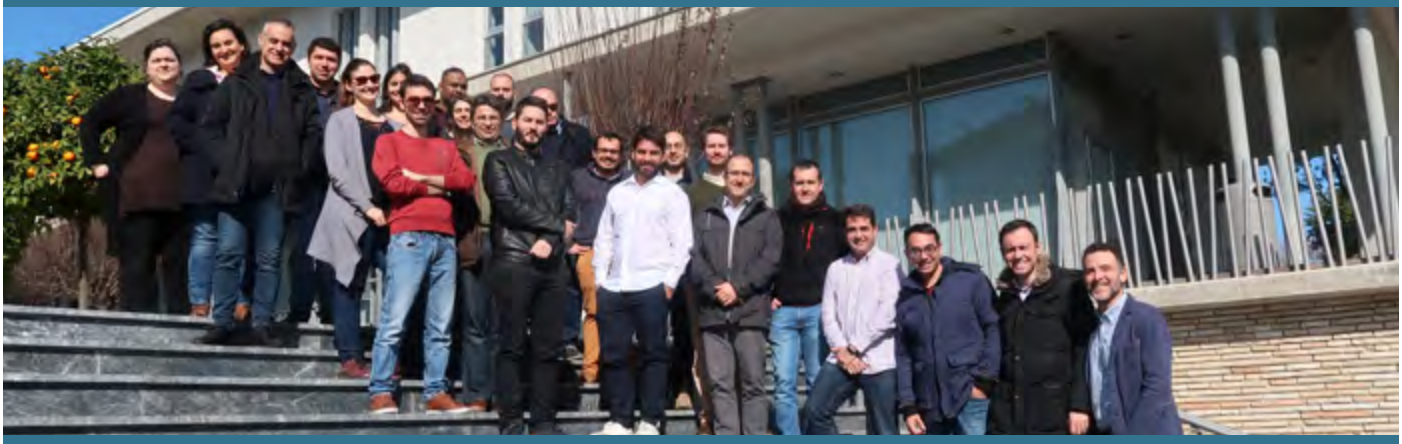
H2020 SYNERGY

The CUREX project participates in a synergy with related EU-funded projects in the field of cybersecurity in the health sector. The main target of this synergy is to identify common problems, discuss about the practices that each project prepares, and establish a joint task force. Apart from CUREX, in this synergy participate the projects: ASCLEPIOS, PANACEA, SAFECARE, SPHINX and FeatureCloud.

In this regard, the CUREX project participated in the ASCLEPIOS project "Security of Healthcare Data-Awareness Workshop" on January 16, 2020 in Amsterdam, the Netherlands. The workshop focused on the current limitations concerning the collection, storage and access to the sensitive patient's medical data and how to solve these.

For more information about the H2020 Synergy CLICK HERE

@CUREX_H2020 curexproject CUREXH2020



Visit our website: www.curex-project.eu
Contact us: info@curex-project.eu

This project has been funded by the European Union's Research and Innovation Program "Horizon 2020" under grant agreement No 826404