2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS)

An overview of the CUREX platform

Antonio Jesus Diaz-Honrubia,
Alejandro Rodriguez Gonzalez
Universidad Politécnica de Madrid (Spain)
E.T.S. de Ingenieros Informáticos
Centro de Tecnología Biomédica (CTB)
Email: {antoniojesus.diaz, alejandro.rg}@upm.es

Juan Mora Zamorano,
Jesús Rey Jiménez
Servicio Madrileño de Salud (Spain)
Instituto de Invest. Sanitaria Puerta de Hierro
Email: {jmora, jrey}@idiphim.org

Gustavo Gonzalez-Granadillo, Rodrigo Diaz
Atos Research & Innovation (Spain)
Cybersecurity Laboratory
Email: {gustavo.gonzalez, rodrigo.diaz}@atos.net

Mariza Konidi
Intrasoft International S.A. (Greece)
Research & Innovation Development
Email: mariza.konidi@intrasoft-intl.com

Panos Papachristou, Sokratis Nifakos
Karolinska Institutet (Sweden)
Dep. Neurobiology, Care Sciences and Society
Email: {panos.papachristou, sokratis.nifakos}@ki.se

Georgia Kougka, Anastasios Gounaris
Aristotle University of Thessaloniki (Greece)
Dept. of Informatics
Email: {georkoug, gounaria}@csd.auth.gr

***Abstract*—Health sector is becoming more and more dependent on digital information every day. This fact can be exploited by cyber criminals who may obtain very lucrative benefits from stolen data. Moreover, a breach of integrity of health data can have terrible consequences for the patients. CUREX project aims to protect the confidentiality of health data and to maintain its integrity by producing a novel, flexible and scalable situational awareness-oriented platform. CUREX has been conceived as GDPR compliant by design. This design has been thought as a decentralised architecture enhanced with a private blockchain infrastructure. Thus, it ensures the integrity of the risk assessment process and of all data transactions.**

***Keywords*-Cybersecurity; Privacy; Health Data; CUREX; Data Exchange.**

I. Introduction

In the last years, with the advent of information technologies to all industry sectors, health data sector has not lagged in this aspect. However, these technologies bring new cybersecurity challenges because of cybercrime. Since healthcare infrastructures are considered as Critical Information Infrastructures, organisations have started to realise the necessity to address these challenges. Compared to other sectors, the most important asset in the healthcare domain is data, which can be a primary target of attack for cyber-criminals. The number of cyberattacks targeting the acquisition of data have recorded a significant rise during the last years.

Therefore, CUREX project [1] is motivated by the current vulnerability of health sector's infrastructures to threats related to privacy and cybersecurity.

The main goal is to build a novel, flexible and scalable situational awareness-oriented platform that can address the protection of the confidentiality and integrity of health data focusing on health data exchange cases.

A healthcare provider can benefit from the CUREX objectives in the following ways:

a) Cybersecurity & Privacy risks: assess the realistic cybersecurity and privacy risks they are exposed to.
b) Optimal Safeguards Strategies: receive recommendations with optimal strategies to address possible risks with safeguards tailored specifically for each healthcare organization profile.
c) Decentralized Blockchain Infrastructure: at its core, a decentralized architecture enhanced with a private blockchain infrastructure ensures the integrity of the risk assessment process and all data transactions that occur between the diverse range of stakeholders involved.
d) Cyber Hygiene Policy Making Strategies: CUREX also places emphasis on improving cyber hygiene through the recommendation of strategies and methodologies for training and raising awareness activities of a healthcare institution's personnel.
e) General Data Protection Regulation (GDPR) [2] Compliant: CUREX is fully GDPR compliant by design.

The reminder of this paper is organized as follows: Section 2 includes the description of the stakeholders who are involved in the CUREX project, Section 3 describes the uses cases in which the project will be deployed, Section 4 gives a high-level description of the CUREX architecture, and Section 5 concludes the paper.

2372-9198/19/$31.00 ©2019 IEEE
DOI 10.1109/CBMS.2019.00042

II. Stakeholders

Stakeholders are defined as the entities that can affect or be affected by the CUREX platform, the support of which is essential for the project success.

- Hospitals: hospitals (and healthcare organizations in general) are organizations hosting and being responsible for most of the individual (patient) healthcare datasets, also used for secondary purposes, such as healthcare quality and performance assessment and biomedical research. Hospitals are responsible for keeping this data safe and protected against unauthorized access.
- Individuals: individuals are the main data providers. They have digital datasets stored in many systems, both outside hospitals, such as social networks, wearables, and inside hospital in clinical data repositories.
- Research Centers: research centers are organizations that use an individual's data, in particular biomedical data, for scientific research purposes.
- Private Businesses and Other Organizations: private businesses are organizations that need an individual's data stored into individual digital accounts and healthcare organizations to execute research and development projects that serve populations' needs. They can be categorized into two types of organizations: (1) industrial research enterprises, such pharmaceuticals and CRO-like companies and (2) commercial enterprises, such Health Management Organization (HMO), Accountable Care Organizations (ACO), and health-tech companies to develop primary care programs and health-tech professional solutions.

A. Stakeholder needs

The main points of the stakeholder's needs that are considered generic and can be supported by evidence in the academic bibliography and/or by surveys. These needs, described below, cover the main groups of stakeholders identified before.

1) Surveys: The CUREX project partner, Karolinska Institute (KI), conducted a survey to support the project objectives and the use cases. This survey was conducted in the requirements gathering phase, eight different expressed needs and requirements stood out and are summarized below. A total of 37 respondents answered, out of them 16 were doctors (45.9%), 9 were nurses (24.3%), 4 were unit directors or CEO/COO (10.8%), 3 were physiotherapists (8.1%), 2 were administrators (5.4%) and 3 were other employees (8.1%) at the two different primary health care centers in Sweden.

a) Privacy: thinking about patient data and Personal Identifiable Information (PII) security in their daily work activities. Respondents rated a median of 5 (on a 7 graded scale).

b) Privacy: perception of information security is an important question in their daily work activities. Respondents rated a median of 5 (on a 7 graded scale).

c) Privacy: their perception of having enough information and knowledge in handling patient data and PII security. Respondents rated a median of 5 (on a 7 graded scale).

d) Cybersecurity & Privacy: most of the respondents rated that different ICT system supports in handling information security is desirable or useful, but not an absolute need or requirement. However, almost 50% of medical professionals state that information about vulnerabilities and cyberattacks/potential theft of patient data is a requirement for them.

e) Cyber Hygiene: only 7 individuals (18.9%) have ever conducted the annual cybersecurity training and web-based certification program DiSA [2], which is mandatory for all employed health care professionals within Stockholm county council.

f) Use Cases: throughout the different answers covering the Use Case scenarios, the need of integration and interoperability of new information security platforms and applications with the present EHR system was observed.

g) Remote EHR Access: few health care professionals had an absolute need/requirement to access the medical record for a foreign visitor but could see the usefulness of this possibility.

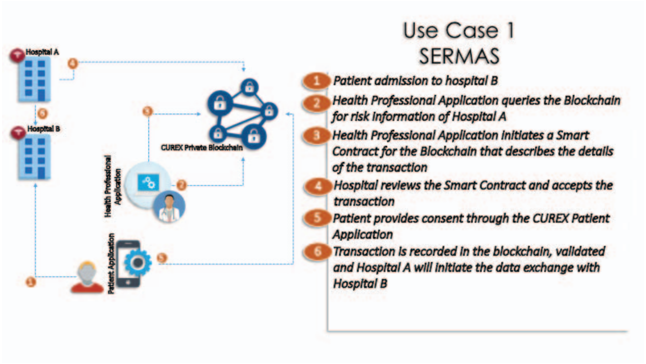
h) Secure mDevices: the majority of respondents wanted to know whether mDevices or wireless POC devices were safe enough to handle and exchange patient data/PII and whether these processes in general are GDPR compliant.

2) Use cases: Following up these results, CUREX needs to develop solutions that are compatible but not limited to the existing heterogeneous digital infrastructures that are already in place. This means that when applying CUREX to SERMAS Hospitals, we need to be aware of the underlying SELENE system, which is the HUPHM's Electronic Health Record (EHR) System. Similarly, the solutions applied to KI need to be aware of Interaktor [3], those tailored to Fundacion Privada Hospital Asil Degranollers (FPHAG) should be aware of SAVAC and the solutions for the third use case need to be aware of the infrastructure developed in the context of MyHealthMyData (MHMD) [4].

3) Data Protection: Protecting patient's data is considered a standard need in the domain of CUREX and therefore a requirement [5].

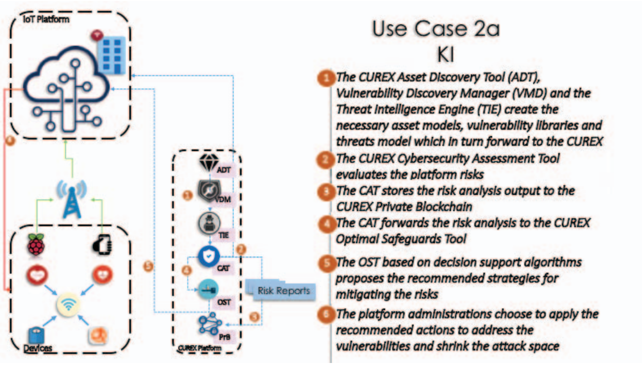
4) Medical Data Sharing: Exchanging patient data to allow (better) remote health services without compromising the security and privacy is considered a standard need and therefore a requirement [6] [7].

5) GDPR: Compliance with GDPR is a legal requirement.



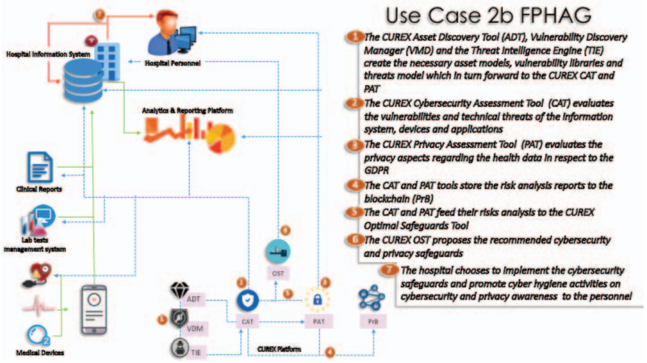
1. Patient admission to hospital B
2. Health Professional Application queries the Blockchain for risk information of Hospital A
3. Health Professional Application initiates a Smart Contract for the Blockchain that describes the details of the transaction
4. Hospital reviews the Smart Contract and accepts the transaction
5. Patient provides consent through the CUREX Patient Application
6. Transaction is recorded in the blockchain, validated and Hospital A will initiate the data exchange with Hospital B

Figure 1. Use case 1 illustration.



1. The CUREX Asset Discovery Tool (ADT), Vulnerability Discovery Manager (VMD) and the Threat Intelligence Engine (TIE) create the necessary asset models, vulnerability libraries and threats model which in turn forward to the CUREX
2. The CUREX Cybersecurity Assessment Tool evaluates the platform risks
3. The CAT stores the risk analysis output to the CUREX Private Blockchain
4. The CAT forwards the risk analysis to the CUREX Optimal Safeguards Tool
5. The OST based on decision support algorithms proposes the recommended strategies for mitigating the risks
6. The platform administrations choose to apply the recommended actions to address the vulnerabilities and shrink the attack space

Figure 2. Use case 2.a illustration.



1. The CUREX Asset Discovery Tool (ADT), Vulnerability Discovery Manager (VMD) and the Threat Intelligence Engine (TIE) create the necessary asset models, vulnerability libraries and threats model which in turn forward to the CUREX CAT and PAT
2. The CUREX Cybersecurity Assessment Tool (CAT) evaluates the vulnerabilities and technical threats of the information system, devices and applications
3. The CUREX Privacy Assessment Tool (PAT) evaluates the privacy aspects regarding the health data in respect to the GDPR
4. The CAT and PAT tools store the risk analysis reports to the blockchain (PrB)
5. The CAT and PAT feed their risks analysis to the CUREX Optimal Safeguards Tool
6. The CUREX OST proposes the recommended cybersecurity and privacy safeguards
7. The hospital chooses to implement the cybersecurity safeguards and promote cyber hygiene activities on cybersecurity and privacy awareness to the personnel

Figure 3. Use case 2.b illustration.

6) User Experience: For software solutions, providing a user-friendly interface is considered a standard need [8] [9] [10].

7) Blockchain Ledger: Having an unmodifiable log with all the professional accesses and use of patients' medical records is considered a standard need [7].

III. CUREX Use Cases

A. Use case 1: data exchange for cross-border patient mobility

This use case, which is illustrated in Figure 1, will be used to set the requirements and validate the CUREX solutions with regards to privacy and risk assessment, validating technical aspects of the CUREX platform, such as the blockchain layer used as a ledger and the end user applications. This will be done in the context of a patient traveling abroad who needs to visit a hospital due to an emergency situation.

In this use case, a patient traveling abroad, from a foreign country, has a medical emergency and must visit a clinic. The patient's Electronic Health Record (EHR) is not available in the visited country. In order to assist, the physician, and help provide a proper diagnosis of the patient's illness, she/he must access the CUREX Platform and get the proper authorization to retrieve the patient's EHR from her/his country of origin.

The main actors in this use case are:

a) A traveler with a medical emergency.
b) A hospital holding the traveler's electronic health record (EHR) in its system, which has been assessed by CUREX.
c) A hospital/care center in a foreign country, also assessed by the CUREX platform.
d) A physician that will attend a traveler with a health emergency.

In the demonstrating scenario, the foreign hospital will be a Swedish clinic. The scenario will demonstrate that it is possible for the physician, who is assisting the Spanish patient, to request and use the patient's EHR. This is done by securely retrieving, transferring and uploading the patient's EHR, from HUPHM's EHR System to the Swedish Clinic's EHRS. The flow should be secure, private, and permanently registered in a non-modifiable (non-malleable) log leveraging the facility provided by CUREX's Private Blockchain.

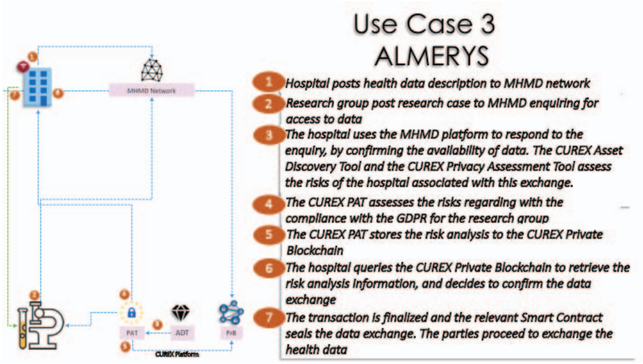
B. Use case 2: data exchange in remote healthcare services

This use case will test and evaluate the CUREX platform potential impact on data exchange in remote healthcare services. This task is split into two subcases:

a) Risk Assessment for an IoT Healthcare Platform, which is visually described in Figure 2, and where the patient's device shares data with the health care center from outside of the hospital/clinic; and
b) Risk Assessment for a Point of Care Systems (POC), which is illustrated in Figure 2, and where the patient's device shares data within the hospital/clinic.

Contrary to the previous use case, the focus now is shifted to modeling and analysing the infrastructure. This is done with a view to deriving risk assessment scores related to privacy and cybersecurity and recommendations about optimal safeguards to be adopted so that the overall cybersecurity and risk levels are enhanced.

In summary, there is a key preparatory phase that is common for use cases 2a and 2b and relates to the CUREX



Use Case 3
ALMERYS

1 Hospital posts health data description to MHMD network

2 Research group post research case to MHMD enquiring for access to data

3 The hospital uses the MHMD platform to respond to the enquiry, by confirming the availability of data. The CUREX Asset Discovery Tool and the CUREX Privacy Assessment Tool assess the risks of the hospital associated with this exchange.

4 The CUREX PAT assesses the risks regarding with the compliance with the GDPR for the research group

5 The CUREX PAT stores the risk analysis to the CUREX Private Blockchain

6 The hospital queries the CUREX Private Blockchain to retrieve the risk analysis information, and decides to confirm the data exchange

7 The transaction is finalized and the relevant Smart Contract seals the data exchange. The parties proceed to exchange the health data

Figure 4. Use case 3 illustration.

Framework installation approach. The CUREX Framework will be installed and integrated in the healthcare's infrastructure; this should include servers, network analysers, etc.

After installing the CUREX framework, the initial cybersecurity and privacy assessment process starts by analysing the hospital's infrastructure. More specifically, after installation, the process will start with the discovery of data assets, services and devices accessing personal data and will end with the analysis and recommendations given regarding optimized cybersecurity and privacy safeguards and cyber hygiene measures. This process will also rank the cyber security and privacy level of the health centers.

C. *Use case 3: data exchange for healthcare research*

This use case, which is depicted in Figure 4, deals with the operation of the CUREX Platform in parallel with the MHMD Platform focusing on compatibility and smooth integration issues.

MHMD is the first European GDPR compliant transactional blockchain platform for healthcare data exchange. It uses a blockchain network to rule data exchanges between hospitals, research centers and other types of institutions within the healthcare sector, thanks to dedicated smart contracts that orchestrate the data sharing lifecycle.

In order to perform a data exchange between two institutions (e.g., Hospital A being the data provider and Hospital B being the data consumer) the Privacy Assessment Tool (PAT) will be used. The PAT will not only evaluate the data package to be shared from Hospital A, but also that Hospital B (the recipient of the data package) possesses the proper safeguards to use the data package. Once the results from the PAT are available in the CUREX blockchain, a query will be performed from the MHMD blockchain to retrieve the risk assessment and, according to the results, trigger or not the exchange of the data package. Since this requires communication between both blockchains, interoperability is needed.

To better assess the risks of sharing data between different organizations, nodes from the MHMD platform will benefit from the CUREX platform when making their final decision about whether sharing or not the data. This final decision will be based on the risk assessment report that they will obtain with the PAT.

IV. CUREX ARCHITECTURE

CUREX is a flexible, modular and scalable situational awareness-oriented platform integrated by a wide range of tools that address comprehensively the protection of the confidentiality and integrity of health data exchange. CUREX architecture allows a healthcare provider to assess the realistic cybersecurity and privacy risks they are exposed to and suggest optimal safeguards for addressing these risks on each business case and application. CUREX is fully GDPR compliant by design. At its core, a decentralised architecture enhanced with a private blockchain infrastructure ensures the integrity of the risk assessment process and of all data transactions that occur between the diverse range of stakeholders involved.

A. *CUREX Layers*

The CUREX architecture defines four different layers needed for the interaction between the CUREX components and health-related parts (e.g. systems of a hospital) to ensure the proper communication among them by defining interfaces and Application Programming Interfaces (APIs), as shown in Figure 5. The design of the architecture follows an agile and iterative approach and uses as input the information from the analysis of the use cases, information of the technologies used in CUREX and the status of actual solutions used in the healthcare domain.

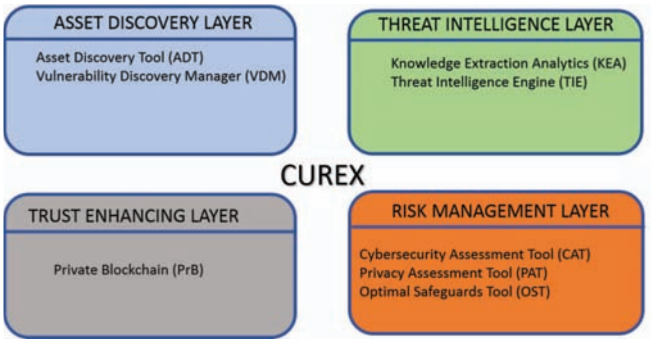

ASSET DISCOVERY LAYER
Asset Discovery Tool (ADT)
Vulnerability Discovery Manager (VDM)
THREAT INTELLIGENCE LAYER
Knowledge Extraction Analytics (KEA)
Threat Intelligence Engine (TIE)
CUREX
TRUST ENHANCING LAYER
Private Blockchain (PrB)
RISK MANAGEMENT LAYER
Cybersecurity Assessment Tool (CAT)
Privacy Assessment Tool (PAT)
Optimal Safeguards Tool (OST)

Figure 5. High-level CUREX architecture.

1) Asset Discovery: The first layer is the Asset Discovery Layer, which will be in charge of discovering all the devices that are connected the hospital's network and try to gather as much information as possible from these devices. The information produced by this layer will be semantic annotated data.

2) Threat Intelligence: The second layer is the Threat Intelligence Layer, which includes the discovery of vulnerabilities and the analysis of various resources that will identify potential threats.

3) Risk Management: On its side, the Risk Management layer involves the analysis and the generation of quantifiable risks that consider both cybersecurity and privacy. It will also provide optimal safeguards and cyber hygiene enhancing techniques based on decision support systems.

4) Trust Enhancing: Finally, the Trust Enhancing layer will include the deployment of a business consensus-based Private Blockchain (PrB) that will store compiled risks reports from the previous layers and will integrate the CUREX tools and end-user applications into a fully GDPR compliant platform.

The PrB will provide a decentralised database to store auditable information such as: activity into the system, risk assessment report, and the data sharing process. As an integral part of the cybersecurity and privacy toolkit, it will be used to record: (a) the cybersecurity and privacy risk scores derived by the relevant assessment methodologies, and (b) all transactions that occur between all stakeholders. Each data exchange request recorded into the blockchain will include a privacy and security risk score. This will provide the essential functionality to audit the process and feed the recalculation process of the risk assessment scores.

B. CUREX Toolkit

The CUREX toolkit will regroup the tools composing the Asset Discovery, Threat Intelligence and Risk Management layers, as depicted in Figure 6. The CUREX toolkit will analyse information coming from the monitoring infrastructure to compute cybersecurity and privacy risk scores associated to the data exchange in the health domain. The toolkit consists of the following tools: Asset Discovery Tool (ADT), Vulnerability Discovery Manager (VDM), Threat Intelligence Engine (TIE), Cybersecurity Assessment Tool (CAT), Privacy Assessment Tool (PAT), and Optimal Safeguards Tool (OST).

1) Asset Discovery Tool (ADT): The aim of the ADT in the CUREX Framework environment is to discover the devices that are within a hospital local network and try to gather as much information as possible from these devices, in order to allow other tools of the CUREX framework to work with the obtained data.

2) Vulnerability Discovery Manager (VDM): The VDM is a domain specific tool for identifying, analysing and reporting vulnerabilities detected in the target system at different layers. The discovery of vulnerabilities is supported by the e-health domain-specific techniques and rules that are created and maintained by experts. They are correlated with historical system data which in turns makes the information of vulnerabilities and recommendations more useful and supports interdependencies between vulnerabilities and the recommended solutions.

3) Threat Intelligence Engine (TIE): The TIE is responsible for the analysis of all threat-related information obtained from the target system at different levels and the (close to) real-time detection of imminent threats, mainly with regards to the safety of data and their exchange with other organisations. The information being analysed includes known vulnerabilities, past incidents, network traffic and system logs which will be monitored in order to timely identify suspicious behaviours and produce alerts.

4) Cybersecurity Assessment Tool (CAT): The CAT is the CUREX platform's implementation of cybersecurity risk assessment. CAT focuses on collecting and analysing cybersecurity events in real time and consolidating a correlation of them for risk assessment. This latter is done together with the e-health business profile (e.g., critical elements, minimum set of functionalities to be provided, impact in the system and services of the threats, etc.). The assessment is performed by contrasting static vulnerability analysis with real time SIEM analysis to support both known and zero days vulnerabilities and attacks.

5) Privacy Assessment Tool (PAT): The PAT is the CUREX platform's implementation of privacy assessment. PAT will provide hospitals and care centres with the appropriate privacy levels in complete alignment with the GDPR directives to protect patients' Personal Identifiable Information (PII) and sensitive clinical data. PAT will perform the necessary analysis on privacy risks based on the modelling of data assets as produced by the Asset Discovery Tool (ADT), and will inform decision makers, based on every business process that concerns the processing and exchange of data, the degree of compliance of the healthcare organisation with the GDPR, by providing an indicative privacy score.

6) Optimal Safeguards Tool (OST): The OST will complement the platform's cybersecurity and privacy risk assessment functionality by proposing optimal safeguards to mitigate the identified as well as future risks emerge in any health data exchange. Its end goal is the organisation to comply with the GDPR Framework.

V. Conclusion

This paper presented the motivation for a secure and private platform for the management and transfer of electronic healthcare data, in a confidential, secure and legally compliant manner.

The main objectives of the CUREX Platform have been exposed, these are: cybersecurity, privacy, a decentralized blockchain infrastructure to assure integrity of the risk assessment and transactions, optimal safeguard strategies and cyber hygiene assessment, all developed under GDPR compliance by design.

The stakeholders and their needs have been identified as well as real documented generic needs, used to gather the platform's requirements.

Three use cases have been presented in 4 different scenarios; each of them addresses a different real-life situation. The scenarios, all together, will validate the different as-

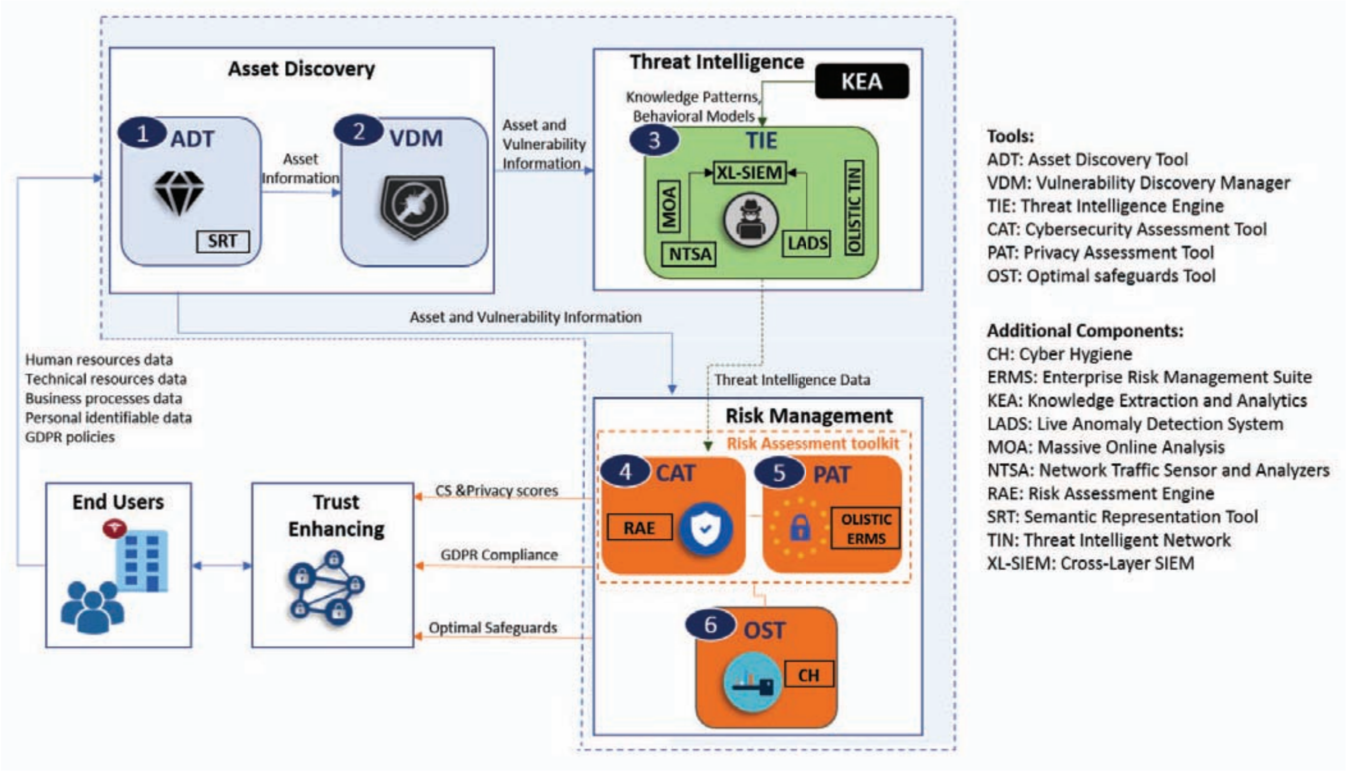

Asset Discovery
1 ADT
SRT
Asset Information
2 VDM
Asset and Vulnerability Information
Threat Intelligence
KEA
Knowledge Patterns, Behavioral Models
3 TIE
XL-SIEM
MOA
NTSA
LADS
OLISTIC TIN
Asset and Vulnerability Information
Threat Intelligence Data
Human resources data
Technical resources data
Business processes data
Personal identifiable data
GDPR policies
Risk Management
Risk Assessment toolkit
4 CAT
RAE
5 PAT
OLISTIC ERMS
6 OST
CH
End Users
Trust Enhancing
CS &Privacy scores
GDPR Compliance
Optimal Safeguards
Tools:
ADT: Asset Discovery Tool
VDM: Vulnerability Discovery Manager
TIE: Threat Intelligence Engine
CAT: Cybersecurity Assessment Tool
PAT: Privacy Assessment Tool
OST: Optimal safeguards Tool
Additional Components:
CH: Cyber Hygiene
ERMS: Enterprise Risk Management Suite
KEA: Knowledge Extraction and Analytics
LADS: Live Anomaly Detection System
MOA: Massive Online Analysis
NTSA: Network Traffic Sensor and Analyzers
RAE: Risk Assessment Engine
SRT: Semantic Representation Tool
TIN: Threat Intelligent Network
XL-SIEM: Cross-Layer SIEM

Figure 6. CUREX Toolkit architecture.

pects, capabilities and overall, the objectives of the CUREX Platform.

The high-level architecture has been presented describing the different layers and essential functionalities of the platform.

CUREX follows an agile methodology, for this reason, all the aspects described in this paper will be under scrutiny and continuous evolution throughout the development of the platform.

Acknowledgment

The research work presented in this article has been supported by the European Commission under the Horizon 2020 Programme, through funding of the CUREX project (G.A. n 826404). Authors would also like to thank all the CUREX consortium members for their work: UPRC, ATOS, ALRS, CLS, INTRA, S5, LEX, 8BELLS, UBI, SURREY, UPM, UCY, AUTH, SERMAS, FPHAG, and KI.

References

[1] “CUREX Horizon 2020 Research and Innovation Action,” https://curex-project.eu/content/deliverables, accessed: 2019-05-20.

[2] “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),” *Official Journal of the European Union*, vol. L 119/1, pp. 1–88, May 2016.

[3] A. Langius-Eklf, M. Christiansen, V. Lindstrm, K. Blomberg, M. Nyman, Y. Wengstrm, and K. Sundberg, “Adherence to Report and Patient Perception of an Interactive App for Managing Symptoms During Radiotherapy for Prostate Cancer: Descriptive Study of Logged and Interview Data,” *JMIR Cancer*, vol. 3, p. e18, Oct 2017.

[4] “MyHealthMyData (MHMD) Horizon 2020 Research and Innovation Action,” http://www.myhealthmydata.eu, accessed: 2019-05-20.

[5] A. Appari and M. E. Johnson, “Information security and privacy in healthcare: current state of research,” *International Journal of Internet and Enterprise Management*, vol. 6, no. 4, pp. 279–314, Oct 2010.

[6] B. Filkins, “Medical Data Sharing: Establishing Trust in Health Information Exchange,” SANS Institute, Tech. Rep., Mar 2017.

[7] ISO/IEC, “Software product evaluation Quality character and guidelines for their use,” ISO/IEC 9126, 1991.

[8] ISO/IEC, “Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs),” ISO/IEC 9241, 1998.

[9] ISO/DIS, “Human-Centred Design Processes for Interactive Systems,” ISO/DIS 13407, 1999.

[10] J. Nielsen, *Usability Engineering*. Morgan Kaufmann, 1993.