SN Computer Science (2022) 3:16
https://doi.org/10.1007/s42979-021-00858-4

ORIGINAL RESEARCH

Risk Assessment Driven Use of Advanced SIEM Technology for Cyber Protection of Critical e-Health Processes

Luigi Coppolino[1] · Luigi Sgaglione[1] · Salvatore D'Antonio[1] · Mario Magliulo[2] · Luigi Romano[1] · Roberto Pacelli[3]

Received: 14 December 2020 / Accepted: 6 September 2021 / Published online: 26 October 2021

Abstract

The approach presented in this paper provides effective protection of critical business processes by applying advanced SIEM technology in a rigorous fashion, based on the results of accurate risk assessment. The proposed SIEM tool advances the State of The Art of the technology along two axes, specifically: privacy and integrity. The advancements are achieved via combined use of two of the most promising technologies for trusted computing, namely: Trusted Execution Environment (TTE) and Homomorphic Encryption (HE). The approach is validated with respect to a real use case of a Smart Hospital (i.e., one where IT is massively used), with challenging security requirements. The use case is contributed by one of the major public hospitals in Italy. Experiments demonstrate that, by relying on continuous monitoring of security relevant events and advanced correlation techniques, the SIEM solution proposed in this work effectively protects the critical workflows of the hospital business processes from cyber-attacks with high impact (specifically: serious harm to or even death of the patient).

Keywords Smart hospital · Security information and event management (SIEM) · Trusted execution environment (TEE) · Homomorphic encryption (HE)

Introduction

With the extensive use of the Internet nowadays, companies are becoming more and more at risk from cyber-attacks. Smart Hospitals are particularly vulnerable, as they lack in cyber security due to time, resource, and knowledge constraints, while focusing more on funding and sustaining their core business. Additionally, from a report of Ponemon Institute [1], reports that "IT security teams are often not effective at communicating cyber security risks to senior management". Also, importantly, risk assessment technologies are not able to cope rapidly with emerging cyber threats, thus leaving a time window where the security of the Smart Hospitals can only rely on the correct behaviour of employees, that nowadays represents the main targets to deliver (e.g., through social engineering techniques) attacks both at IT level (i.e., malware) as well as at human level (e.g., CEO frauds) that may severely compromise businesses activities.

Real-time security monitoring includes a handful of technologies, with Security Information and Event Management (SIEM) being one of the key building blocks. SIEM solutions [2–4] typically correlate, analyse, and report information from a variety of data sources, such as network devices, identity management devices, access management devices,

Luigi Romano is also an Associate Researcher at the ICAR institute of the Italian National Research Council.

This article is part of the topical collection "Advances on Signal Image Technology and Internet based Systems" guest edited by Albert Dipanda, Luigi Gallo and Kokou Yetongnon.

✉ Luigi Sgaglione
luigi.sgaglione@uniparthenope.it

Luigi Coppolino
luigi.coppolino@uniparthenope.it

Salvatore D'Antonio
salvatore.dantonio@uniparthenope.it

Mario Magliulo
mario.magliulo@ibb.cnr.it

Luigi Romano
luigi.romano@uniparthenope.it

[1] Engineering Department, University of Naples "Parthenope", Naples, Italy

[2] Institute of Biostructure and Bioimages, National Council of Research, Naples, Italy

[3] Radiation Oncology Department, University "Federico II" Hospital, Naples, Italy

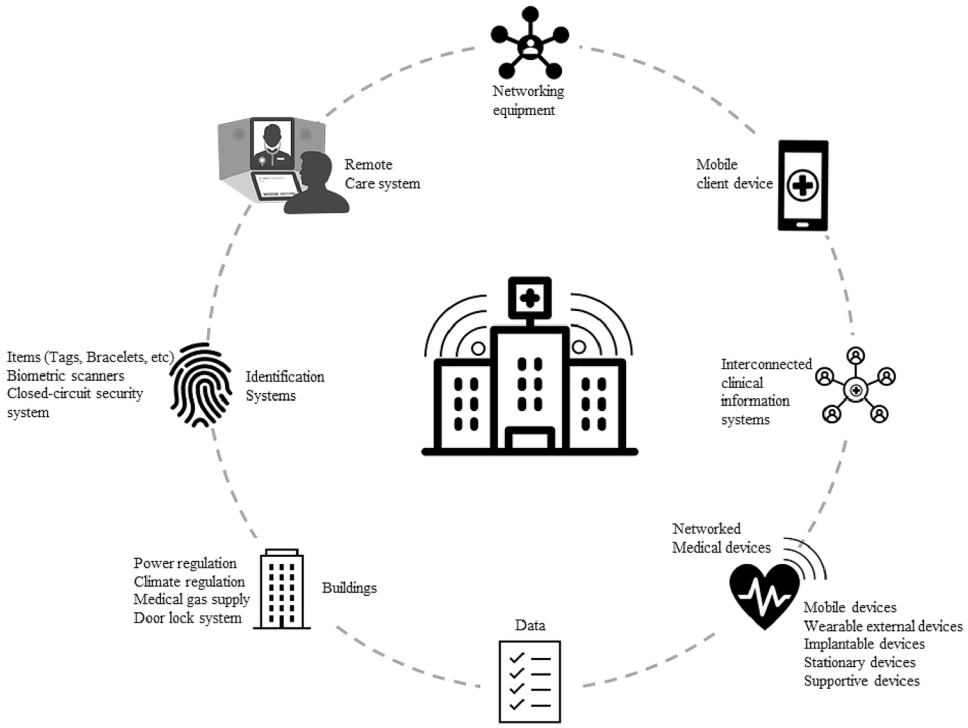

Fig. 1 ICT-based assets in a smart hospital

and operating systems. Point SIEM products provide useful data but they lack visibility across a broader set of security elements needed to detect the increasing number and variety of cyber-attacks on corporate and government enterprises.

This paper proposes an effective risk assessment approach and an associated SIEM tool for addressing some of the top priority security challenges experienced by "Smart Hospitals", as defined by ENISA in [5]: "A smart hospital is a hospital that relies on optimised and automated processes built on an ICT environment of interconnected assets, particularly based on Internet of things (IoT), to improve existing patient care procedures and introduce new capabilities".

The research work is driven by a challenging use case, contributed by a large public hospital in Italy, involving a wide variety of ICT based assets and processes and directly linked to large patients' communities. This ensures that the approach has a strong research and innovation capability, and is well focused and of direct relevance to the Smart Hospitals context. The use case focuses on a critical business process of the hospital, specifically the radiation oncology workflow. It provides a comprehensive set of security challenges, which collectively results in a strong safety case from the patients' point of view. As such, it constitutes an extensive reference scenario both for the definition of the requirements and for the validation of the results. With respect to this use case, we identify life threatening attack scenarios and analyse how real-time monitoring—as provided by our SIEM solution—can help counter those attacks. The use of ICT enables Smart Hospitals to deliver a richer service offer at a higher level of quality, but it also dramatically enlarges the attack surface [5]. The number and the variety of ICT-based assets are huge, as schematically represented in Fig. 1.

Each individual asset has a large attack surface, resulting in the exposure of the ICT infrastructure of the Smart Hospital to a wide variety of cyber-attacks. Evidence in [6] demonstrates that many medical systems are exposed to the Internet, and that they can potentially jeopardize critical data such as patients' Personal Identifiable Information (PII) and medical records. The number of unsecure medical devices is an urgent and dramatic societal issue, that the proposed approach takes in due consideration. The 2017 RSA conference highlighted 170 million connected devices discovered using the Shodan search engines across 10 US cities, including unprotected medical devices.

The work presented in this paper builds on and extends authors' previous research described in [7]. In our conference paper, we presented the basic idea, mainly in terms of ambitions and conceptual functions.

This paper makes three new key contributions.

First, we explain how the risk assessment phase can be used by the Chief Security Officer (CSO) of the hospital to identify the most critical business processes, i.e., those where a security breach may result in major impacts on patients' health (or even result in death).

Second, we describe in detail the current version of the SIEM prototype which implements the proposed approach. This also includes a concise—yet self-contained—treatment of the key enabling technologies.

Third, we present the results of a thorough experimental campaign conducted in the last months. Experiments were done with direct involvement of end users and demonstrated in relevant environments, which enabled us to achieve quite a high Technology Readiness Level (namely: TRL6).

The proposed SIEM solution protects company investments in cyber security, since it can seamlessly interoperate with COTS (Commercial Off-The-Shelf) security solutions from major vendors, as well as with best of breed Open-Source products which could have already been deployed on the infrastructure.

Also, importantly, the proposed SIEM solution is designed for use in a federated environment with multiple levels of hierarchy, possibly distributed across multiple countries, relying on a modular offering of composable micro-services. The main motivations for choosing the microservices architecture rely in its modular characteristics, which lead to flexibility, scalability, and reduced development effort. This facilitates the adoption of widely recognized best practices for security improvement, namely: separation of duties and least privilege principles.

Smart Hospitals are sensitive infrastructures due to their criticality for people's well-being and safety. Health plans, lab data, and medical machinery are examples of valuable assets that digitization, systems interconnectivity, and IoT technology make more and more exposed to cyber threats.

A fully-fledged prototype of the SIEM has been developed, based on the specific requirements of the Smart Hospitals' context, and customized for the protection of critical business processes. The SIEM prototype has been empowered with an innovative solution for secure data exchange and processing. The result has been validated by end users and demonstrated in relevant environments, thus achieving TRL6.

The Security Improvement Process

Today's sophisticated and frequently changing threat landscape requires a brand-new way of performing risk management. Composition of multiple services, interconnection between different infrastructures, use of COTS technologies, virtualization and migration to the cloud computing paradigm are some of the factors that make the Smart Hospital's environment extremely dynamic. In this scenario static risk management methodologies prove to be inadequate, and uncertainty rises over time. Therefore, the need arises to rethink risk management and make it capable of considering these changes in order to be accurate when estimating risks and effective when selecting treatment strategies.

To meet this requirement the proposed SIEM system cycles in a human supervised closed loop, where information is continuously extracted from the target system (as well as from external sources providing information that is relevant for risk management purposes) and processed for implementing continuous and adaptive risk assessment as well as effective risk treatment.

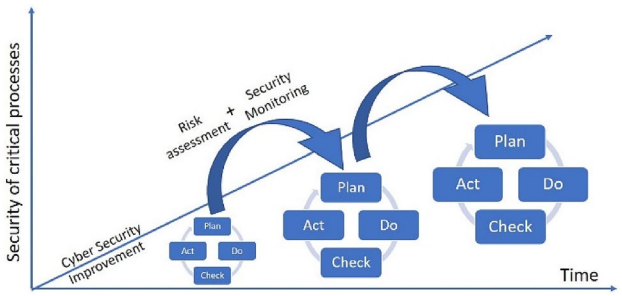

Fig. 2 Cyber security continuous improvement process

Risk assessment is a process that is made up of three processes: risk identification, risk analysis, and risk evaluation. Risk assessment is commonly considered part of the risk management process. While risk management is usually meant to be a continuous process, risk assessment is traditionally assumed to be executed at discrete time points. A common approach (to which all existing products conform) is to run it periodically (e.g., once per year) or on an event-driven base, that is whenever the considered infrastructure undergoes changes that can significantly impact the actual level of risk to which the system is exposed. In complex systems, like a Smart Hospital, composed of a high number of heterogenous devices and characterised by interdependences with non-IT components, very frequent changes in the infrastructure perimeter occur. These considerations imply that even daily execution of risk assessment procedures might be largely ineffective and thus lead to the conclusion that risk assessment should be (1) a continuous process, and (2) it should be based on criteria and assumptions that are dynamically adapted to the status of the Smart Hospital to be protected.

The proposed risk assessment approach (Fig. 2) enables Smart Hospitals to do a thorough analysis of vulnerabilities and failures through an integrated approach that considers both technical and technological aspects related to medical devices, and organizational and human factors related to the various stakeholders (including medical professionals, health care providers, and insurance providers). By doing so, Smart Hospitals can effectively improve their cyber security level, in a continuous process, as illustrated below. The proposed approach innovates at the technological level and at the process level—an important dimension in engaging Smart Hospitals' employees in the improvement of cyber-resilience. At the technological level, the approach innovates monitoring and protection technologies (as well as other security enhancing technologies,

which are not discussed in this paper). At the process level, it improves the security of Smart Hospitals' e-Health services, introducing innovations in the tracking back from data breach to originating channel, enhancing the security process to immediately react based on this improved tracking. It is worth emphasizing that the proposed approach directly supports five of the specific imperatives listed in the Report On Improving Cybersecurity In The Health Care Industry—Health Care Industry Cybersecurity Task Force [8], specifically:

- Imperative 2—Increase the security and resilience of medical devices and health.
- Imperative 3—Develop the health care workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities.
- Imperative 4—Increase health care industry readiness through improved cybersecurity awareness and education.
- Imperative 5—Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure.
- Imperative 6—Improve information sharing of industry threats, risks, and mitigations.

In the proposed approach, we measure: (a) the exposure of each Smart Hospital to most relevant cyber threats in the HC sector, (b) the privacy risk related to the processing of personal data by Smart Hospitals and (c) the effectiveness, over time, of the training and awareness methods adopted by the institution to reduce the above exposure.

Concerning the exposure of each Smart Hospital business process to cyber threats, the assessment procedure considers the most common assets and threats for Smart Hospitals. This will also include input about the risk evaluation criteria and methodologies from the cyber-insurance market, as well as the inputs from domain experts and existing surveys. The calculation of the risk profile will therefore consolidate input from different sources in the Smart Hospital system, mainly.

- At the IT level: the information about assets (including data and IoT devices) and events (security alerts and warnings) coming from the Monitoring and Protection tools installed in the hospital network. This information will allow to adapt the level of risk based on the status of the local network (e.g., elevating risks when alerts/warning are detected at the IT level).
- At the Human level: the status of the cybersecurity training, and the related assessments. This information will allow to define the risk profile also considering the ability of the hospital staff to face cyber threats (especially those based on Social Engineering techniques).
- At the Organizational level: the set of processes and solutions already in place to protect major assets of the Smart Hospital. This information can be used to refine the risk level (e.g., lowering it in case specific solutions are in place to protect against specific risks).

The collection of relevant information is automated to the largest possible extent (depending on the level of digitalization of each Smart Hospital). This is an important feature, since the level of automation in the collection of information heavily impacts on the "freshness" of the information itself, thus on the quality of the risk profile generated by the tool, and on the frequency of the risk re-assessment.

Concerning the profiling of privacy risks, i.e. that personal data are not managed in accordance to GDPR principles, the approach will define the overall level of risk of the hospital based on accurate assessment of individual risk, by relying on three inputs: (a) the personal information managed by the hospital, (b) how the personal information is handled, stored and processed, (c) the level of knowledge, in GDPR and cybersecurity, of people handling personal data in the Smart Hospital.

The outcome of the continuous risk assessment process is used by risk treatment to select the most suitable option.

Risk treatment is a risk modification task, which involves selecting and implementing one or more treatment options. Once a treatment has been implemented, it becomes a control, or it modifies existing controls. Since there are many treatment options, risk treatment involves activities such as risk transfer, risk retention, risk avoidance, and risk reduction. The proposed SIEM provides risk treatment features that enable to select—in a timely fashion and based on based on a consistent and constantly up to date view of the system to be protected—the most appropriate strategy for treating the risks to which the Smart Hospital is exposed. The SIEM system oversees automatically selecting the most appropriate risk treatment strategy according to the identified risks and to their potential impact.

A human operator (the Security Officer) is given the possibility of steering—and even of overruling—the decision made by the SIEM system. The final decision that will be made by the human operator will also consider the results of studies that will be conducted (as an integral part of the activity of the project) on cyber-insurance models and audit tools for managing the interplay between IT security investment and cyber-insurance.

It is worth emphasizing that the proposed approach favours compliance to current and upcoming regulations, and in particular: the Medical Devices Directive 93/42/EEC; the General Data Protection Regulation (GDPR) 2016/679; the Privacy and Electronic Communications Directive 2002/58/EC and the upcoming regulation foreseen for implementation in 2019; and the Cross-border HC Directive 2011/24/EU; all of which confer several articles on data protection and security.

Advanced SIEM Support

The risk assessment phase described in "The Security Improvement Process" enables the Chief Security Officer (CSO) of the hospital to identify the most critical business processes, i.e., those where a security breach may result in major impacts on patients' health (or even result in death). To protect critical business processes, a customized Security Information Event and Management (SIEM) solution has been developed—i.e., specifically tailored to the needs of hospitals and health care institutions—with advanced data processing and event correlation capabilities. The results of the processing provide timely and accurate information about cyber-attacks, as well as directions for countering them and actions for mitigating their effects. To protect previous investments, the SIEM interoperates with market solutions from major vendors (that might have already been installed).

Since cloud computing is an emerging trend in the ICT strategy of companies whose core business in not ICT, a larger and larger fraction of health organizations (which include Smart Hospitals) is progressively moving to the cloud), the proper approach and accompanying SIEM tool is.

- "Cloud-enabled"—Meaning that it is designed and implemented considering issues, constraints, and aspects that are specifically related to cloud technology (e.g., SIEM monitoring features will gather events/data not only at the Operating System level, but also at the Virtual Machine level).
- "Cloud-ready"—Meaning that it will be possible to seamlessly deploy the SIEM on the cloud (e.g., larger organizations with a stronger IT department might opt for a traditional setup on a standard IT infrastructure, or on private cloud, while smaller ones might prefer a public cloud from an external provider).

It is worth emphasizing that not only the SIEM enables effective protection from cyber-attacks with higher impact (meaning: which might well result in serious harm to or even death of the patient), but it also supports careful planning of risk transfer strategies for residual risks.

Conceptual Architecture

The conceptual architecture of the SIEM solution which we propose in this paper was inspired by the SIEM solution [9] developed by some of the authors within the context of the KONFIDO project, which focused on secure exchange of clinical data in a cross-border setup. The architecture of the KONFIDO SIEM was customized for an intra-enterprise setup, based on the results of a detailed requirements analysis of the specific security needs and environment constraints of smart hospitals.

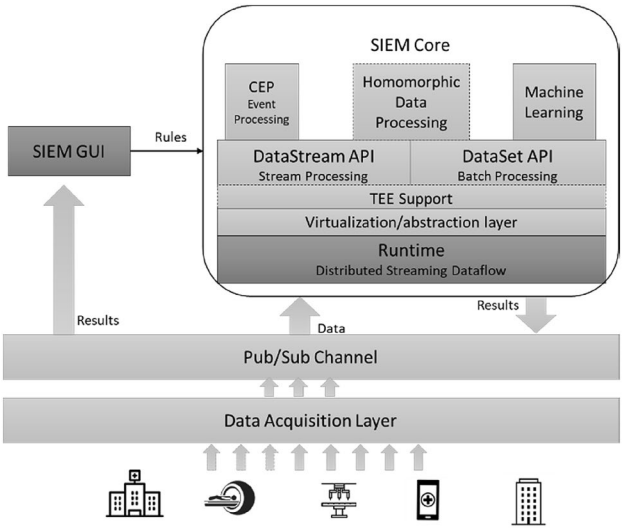

Fig. 3 Conceptual architecture of the proposed SIEM solution

The new architecture effectively integrates in a microservices based organization the following key components/features (Fig. 3):

- Two data processing APIs—One for stream processing and one for batch processing. The availability of these two complementary features is essential for spotting anomalous events and/or event patterns in a timely fashion. Importantly, batch processing features make context/domain knowledge available to stream processing features for spotting deviations of observed events/values from what is known to be normal/acceptable.
- Homomorphic operators—To process data directly in homomorphically encrypted form, i.e., without decrypting it before the computation phase. By doing so, data is never exposed to the external world in plain text form.
- A Trusted Execution Environment (TEE) support layer—To enable protected execution of security critical functions on data which must necessarily be in clear.
- A virtualization/abstraction layer—To facilitate use of TEE support by higher software layers.
- A data acquisition layer—To gather, parse, filter security-relevant events/data. It includes a variety of specific functions, to efficiently collect security relevant events from medical devices and applications.

It is worth emphasizing that the integration of TEE technology, combined with the ability of processing data in Homomorphically encrypted form, results in superior

protection of data confidentiality, in all phases of the data cycle, including "data in use", which is unarguably the most critical one.

To address the perceived disadvantages of automation (e.g., loss of control, lack of trust, fear of change), we take a Human In the Loop (HIL) approach, to allow for judgment and knowledge-based decisions, which allows humans to override automated system decisions and thus ensures that the end-users retain, if they so wish, full control of the platform always.

Enabling Technologies

Homomorphic Encryption

Traditional cryptography (e.g., AES, RSA) makes an effective tool for protecting data while being transmitted and/or at rest. Unfortunately, it does not offer any kind of protection during data processing since data elaboration requires its decryption and thus the exposition of plaintext.

Unlike traditional cryptography, Homomorphic Encryption (HE) schemes allow to perform computations on ciphertext by obtaining results whose decryption would match the output achieved if the operations had been performed on the unencrypted data.

HE allows entities to delegate the processing of their data to untrusted third parties, or untrusted parts of the system, without never exposing the plaintext and thus without threatening data confidentiality.

The most interesting HE schemes are the so called Fully Homomorphic Encryption (FHE) [10] which are defined as a lattice, thus introducing both homomorphic multiplication and addition, and so enabling virtually any kind of homomorphic processing.

Fully HE schemes present two main drawbacks: (1) Cipher Text Expansion (CTE) [11], that is a huge increase in size of the ciphertext with respect to the plaintext, and (2) performance penalty. The actual amount of both special and temporal penalties depends on some security parameters and the actual scheme adopted for the implementation. As an example, in a Logistic Regression Model on encrypted data developed by Microsoft Research [12] using their homomorphic library SEAL [13], 1 Mb of plaintext was resulting in more than 10 Gb of encrypted data, an addition was still consuming under 1 ms, whereas a multiplication required over 5 s.

To make practical HE, thus limiting the related penalties, the concept of somewhat Fully Homomorphic Encryption (FHE) scheme was introduced [14]. In HE the security of the system is based on some redundancy introduced into the ciphered text. Every time the ciphertext gets manipulated some noise is introduced reducing the available redundancy. When the noise consumes the whole redundancy, the ciphertext becomes un-decryptable. Practically speaking this means that only a predefined number of elaborations is possible. Fixing lower redundancy, while limiting the processing capability, also reduces the mechanism penalty. Our choice was to use the library TFHE [15] since it provides a good compromise between performance penalty and functionalities. Moreover, since it is fully implemented in C, it was fully possible its porting in an SGX environment [16].

Trusted Execution Environment

As for the Trusted Execution Environment (TEE) technology, the proposed SIEM relies on Software Guard eXtensions (SGX) [17–19], an Intel architecture extension designed to increase the security of application code and data.

According to Intel[1], SGX "offers hardware-based memory encryption that isolates specific application code and data in memory. Intel SGX allows user-level code to allocate private regions of memory, called enclaves, which are designed to be protected from processes running at higher privilege levels".

The secure enclave prevents any process running outside—even a privileged one—from accessing or modifying the protected address space. Protection mechanisms are based on encryption and hashing algorithms, are transparent to the users, and enforced by the processor. An interface—defined in a domain-specific C language—is declared by the programmer to establish entry points, i.e., calls to/from an enclave (namely ECALLS and OCALLS).

Another key feature provided by SGX is remote attestation. Remote attestation allows a hardware, or combined hardware/software, entity to establish a trust relationship with a remote party. Specifically, it enables to verify if a remote software is running inside an enclave, if such an enclave is managed by an SGX system updated to the latest security level, and if any software tampering happened.

The main cost of SGX adoption is in terms of performance penalty [20], especially due to the cryptographic operations necessary to enter and leave the enclave. Moreover, the size of the Enclave Page Cache (EPC) used to store protected code and data, is limited to the Processor Reserved Memory (PRM) (128 MB) allocated by the BIOS at boot-time.

Open Source and COTS Software

The SIEM has been built using best of breed Open-Source technologies, and in particular.

[1] https://www.intel.co.uk/content/www/uk/en/architecture-and-technology/software-guard-extensions.html.

- Apache Flink—It is a distributed processing engine for the stateful computations over unbounded (have a start but no defined end) and bounded (have a defined start and end) data streams [21].
- Apache Storm—It is a distributed real-time computation system for processing unbounded streams of data, which does for real-time processing what Hadoop did for batch processing. It can be used with multiple programming languages and integrates with virtually any queueing and database technology [22].
- Esper—It is a tool for complex event processing (CEP) and streaming analytics, which enables rapid development of applications that process large volumes of incoming messages or events (both historical and real-time). It filters and analyses events in a variety of ways and responds to conditions of interest [23].
- The ELK Stack—This includes Elasticsearch, Kibana, Beats, and Logstash. These tools enable collection of data from virtually any source, in any format. The collected data can then be analysed and visualized in real time [24].

The virtualization/abstraction layer which facilitates the use of the TEE by upper layers, is built using the following technologies.

- The Java Native Interface (JNI): a native programming interface that is part of the Java Software Development Kit (SDK). JNI lets Java code use code and code libraries written in other languages, such as C and C++ [25].
- SCONE: enables secure execution of containers and programs using intel SGX. It can transparently encrypt files and network traffic, to protect data from unauthorized access (even by privileged software, such as the operating system or the hypervisor) [26].
- Graphene-SGX: Graphene is a library OS for Linux multi-process applications [27]. It is much lighter weight than running a complete guest OS in a virtual machine (VM). In the current implementation of our SIEM, we used Graphene to provide Intel SGX support to SIEM components.

To distribute events among SIEM components, the current implementation uses Apache KAFKA [28] and Apache ActiveMQ [29]. The SIEM also integrates external data sources and correlates external information to events related to the status of the infrastructure. External data feeds include threat intelligence sources, which enable the SIEM to timely spot anomalies, and suggest recovery actions. Importantly, the correlation logic is based on detailed knowledge of the Business Process.

Experimental Campaign

We validated our approach through a substantial use case, on the protection of a critical workflow that also integrates data from wearable sensors.

Description of the Business Process

The validation campaign took a user centric approach, driven by the real challenges that Smart Hospitals must address.

Radiotherapy implies a chain of several interdependent actions that are based on sophisticated computer technology. The goal is the accurate treatment of patients via reliable and efficient planning of actions. This workflow is driven by several digital steps orchestrated by a "record and verify" system. The chain starts with the acquisition of patient data (stored in medical records) and ends with the delivery of the treatment (which entails direct control of active medical devices). In between, we have: (1) image acquisition of the body section involved by the disease by computerized tomography (CT simulation); (2) transfer of the acquired images to the contouring station; (3) delineation of the volume of interest (target and organs at risk); (4) prescription of the treatment by the radiation oncologist; (5) transfer to treatment planning system; (6) planning by the physicist; (7) approval by the physicist; (8) approval by the radiation oncologist; (9) transfer to the treatment machine console; (10) set up and treatment verification with the patient; (11) approval of the radiation oncologist; (12) start of the radiation therapy (Fig. 4).

In the case of patients who can also benefit from chemotherapy, the system can directly control a robotic arm for chemotherapy preparation. Many Smart Hospitals (including Azienda Ospedaliera Universitaria Federico II) are endowed with computerized systems able to set-up chemotherapies in a totally automatic way starting from the work lists sent by the dispatchers. These systems can weigh active ingredients and solutions, reconstituting powdered drugs, dosing the components using a mechanical robotic arm and dedicated actuators, setting up syringes, bags, infusion devices, unloading the materials used with maximum safety for the preparatory technician. The adoption of such systems brings many advantages: patients are protected by latest-generation technological solutions such as a barcode-based labelling system for total traceability; the absolute hygiene is guaranteed by an ISO 5 self-contained chamber (in accordance with ISO 14644); the staff is protected from accidental exposures by limiting the interaction with high-risk drugs only to the loading and unloading of the objects, etc. However, since the system

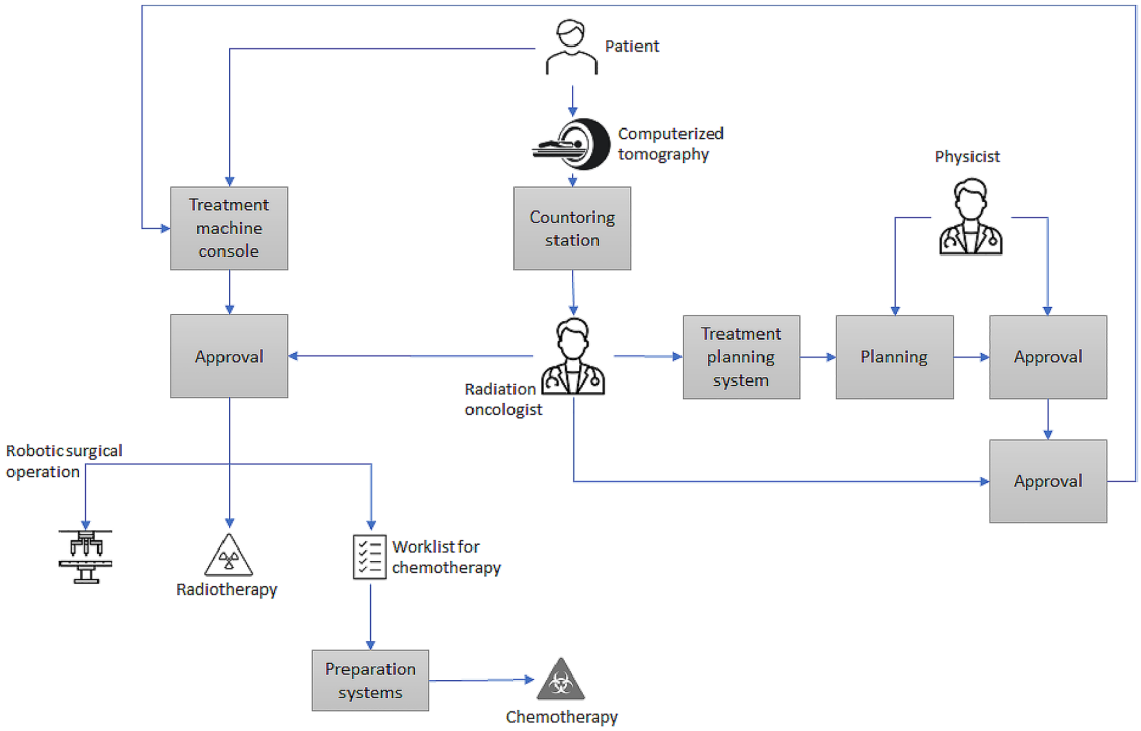

Fig. 4 Radiation oncology process

is inserted in a workflow, where several ICT devices are connected and communicate through the network, it is exposed to cyber-attacks. Securing these systems is of a paramount importance since the impairment of the correct functioning of the system resulting from an attack could cause tragic consequences to patients, including death.

For specific types of tumours, a surgical robot can be used to remove it, as a complement to the radiotherapy treatment. The Smart Hospital contributing the use case has the da Vinci surgical system, a robotic surgical system which is commonly used for prostatectomies, and increasingly for cardiac valve repair and gynaecologic surgical procedures. Our solutions will also protect the data and control flow to/from this surgical robot.

To improve the quality of the care process of patients undergoing radiation therapy, information about patients' health is also collected when patients are at home. The collection process relies on Activity Tracker (ACT) and Bluetooth (BT) technology. Activity Trackers, also known as Fitness Trackers, turned out to be suitable for biometric monitoring in environments other than fitness, and in medical setups. Recent devices are equipped with biometrical sensors which can monitor and record key biometric parameters—such heart rate, galvanic skin response, skin temperature, sleep cycle, and motion using a high precision 3-axis accelerometer. Some trackers have a built-in altimeter or other sensors on the shoes, which provide accurate information about the activity of the monitored person. A key advantage of these technologies is the possibility of collecting data in a non-invasive way, to gain insight about the patient life at home. This data can help the radiation oncologist to better understand the impact that the radiation therapy treatment has on the patient when he/she is outside of the hospital. As importantly, this type of monitoring enables the detection—and in some cases the prediction—of emergency situations which can have a negative impact on the quality of life of the patients. As an example, it enables the detection of falls. The frequency of falls dramatically increases not only in older (in older people, falls represent a major health problem, that in western countries has been estimated to affect about one third of people aged 65 and over) or dementing people (especially when the motor behaviour is compromised such as in wandering) or people with cognitive decline, but also in patients undergoing invasive treatments, such as radiotherapy, which result in weakness and reduced responsiveness. The consequences of falls are disability, reduced quality of life and financial costs to individuals and society. Falls have varied and complex implications such as social withdraw, anxiety and depression, and an increased use of medical services. About 20% of falls require medical intervention and 5–10% provoke a fracture. According to recent estimations (SINIACA) the unit cost per hospitalization from falls in domestic environment

is approximately 3.000 Euros, causing a burden of approximately 400 million euros per year.

The use case therefore provides an overall critical and extensive workflow, creating an information chain involving data, advanced and very sophisticated devices, and the use of wearable sensors originated from the fitness world, and whose potential level of compromise is high. It also creates this chain across local and diverse remote locations.

It is also worth emphasizing that the use case includes the top six of the eight most critical categories of assets in Smart Hospitals, as per ENISA's classification in [5], and specifically.

- Networking equipment.
- Interconnected clinical information systems.
- Data.
- Networked medical devices.
- Mobile client devices.
- Remote care systems.

It is important to note that within these categories, some of the assets are mainly used as vehicles to channel attacks, while others will mainly be a target of a cyber-attack and others must be considered both as a target and as a vehicle.

When designing the attack scenarios, we targeted all the six asset categories, namely: (1) "Diagnostic & monitoring equipment" (the top category in terms of purchases by Healthcare Delivery Organisations (HDOs), with 68%); (2) "Networking equipment designed specifically for medical needs" (the top category in terms of device makers, with 56%); (3) radiation equipment; (4) wearable devices; (5) mobile medical applications; (6) robots.

Notably, in the risk assessment phase the criticality of devices was taken in consideration, based on their active/passive behaviour.

- Active medical devices (AMD) are those devices that interface directly with a patient and administer some medical treatment, which in the event of a compromise could adversely affect the patient's health. If a device is modified to fail to deliver the necessary treatment, a patient could die or suffer serious injury.
- Passive medical devices (PMD) are devices that report on patients' vital parameter values or other information needed to inform or alert clinical staff of medical events or needed treatment. If these devices are compromised, they could affect patient health through a clinician by reporting false information. If incorrect information is reported to clinical staff, they are more likely to make life-threatening decisions regarding patient treatment, such as not addressing a condition or applying the wrong treatment.

Fig. 5 Radiation treatment workflow

Attack Scenarios

The selected attack scenarios refer to safety critical phases of the radiation oncology process. The Radiation Oncology Department is a highly digitalized sector of the hospital infrastructure, which makes its business processes particularly exposed to cyberattacks. The workflow related to a patient treatment in the Radiation Oncology Department is represented in Fig. 5.

The first step of the radiation treatment consists in the computed tomography (CT) scan of the region of the patient to be treated (1). At this stage Fiducial Markers (e.g., reference points) visible on the CT scan are identified. Images are thus transferred to the contouring system where the physician delineates the volumes of interest (target of the treatment and organs at risk) (2). Then these images are sent to the Treatment Planning System (TPS) where the physicist defines and simulates the treatment (3). The resulting plan is revised for approval by the physician at stage and transferred to the Record and Verify system (4) that oversees controlling the linear accelerator (linac) applying the treatment (5) (Fig. 5).

We focused on two attack scenarios, which are described in detail later in this section. The scenarios were chosen for two main reasons.

1. They have high impact; since the components which are attacked implement critical functions, a cyber-attack which affects their operation is likely to have major impacts on the correctness of the treatment and ultimately on the health and/or on the quality of life of the patient.
2. They are related to a large attack surface; the attack vectors are the output of the CT study and of the TPS study, which collectively represent more than 90% of the total file volume of the department.

First Scenario: Attack to the Contouring System

A cyberattack is launched against the contouring system, whose purpose is to define morphologically and physically: (1) the target of the treatment (which must be exposed to radiation), and (2) the organs at risk (vital organs which should not be exposed to radiation). The contouring system is connected to the hospital LAN. Protection against unauthorized access is implemented via weak authentication, based on individual credentials. This attack scenario

assumes that an attacker gains access to the system (e.g., by stealing/guessing the credentials of a legitimate user) and modifies contouring delineations, thus altering the morphological information before it is sent to the TPS. An alteration of the contouring system output, if delivered to the TPS, would result in an incorrect treatment and possibly in serious damage to the patient.

Second Scenario: Attack to the R&V System

The target of the cyberattack is the R&V system, where the data of the treatment plan as well as the numerical description of monitor units of radiation are processed. Specifically, patient's clinical data and the radiation treatment plan, including beam orientation and dose delivery, are used by the R&V system to control the linear accelerator. The output of TPS includes different files, and in particular the output Dose Map and the RTPlan. The total size of these files is less than a few MB (typically <5). Since the files contain information on which the plan is based and critical data that allows LINAC setting and dose control, an attack to the integrity of the data could result in dramatic consequences to the patient.

Should an attacker manage to access the R&V system, he/she could maliciously change treatment parameters—e.g., the power of radiation delivered to the patient—which could even kill the patient.

Experimental Results

In this section we discuss how the proposed SIEM system can be used to timely detect cyber-attacks, and thus prevent the occurrence of cyber-incidents with high impact. The purpose of the experiments is to demonstrate that the SIEM can cope with the hard real-time constraints of the use case. The analysis is done with respect to the two aforementioned scenarios, whose characteristics are representative of a wide class of attacks.

The SIEM system uses both anomaly-based and signature-based techniques to spot deviations between the expected values of the radiation treatment process parameters and the ones received by the system components to perform treatment process.

Correlation-based attack detection is carried out by processing homomorphically encrypted data in a trusted execution environment, thus ensuring confidentiality and integrity of sensitive data and preserving patients' privacy.

Compositions of different operators are used to execute native or homomorphic encryption-based analytics on collected datasets for signature-based or anomaly-based attack detection.

With reference to the first attack scenario, the SIEM system processes the output of the contouring system and uses it as indicator of compromise to detect modifications of the contouring delineations with malicious values.

Each radiotherapy system produces files according to the DICOM RT standard. More precisely, contouring profile is saved in a text format that specifies regions of interest using spatial coordinates (x, y, and slice number). The size of these files is around 1 MB and the format is plain text. These characteristics make it very easy to change file contents. Conversely, the data size did not allow straightforward use of homomorphic encryption. It is indeed a well-known fact that the capability of HE to process data without decryption comes at the cost of a dramatic increase in the size of the encrypted data (phenomenon which is referred to as Cipher Text Expansion (CTE) [30]. CTE is a major limitation of HE. To reduce the effects of ciphertext expansion, we had to implement a feature extraction pre-processing stage in the SIEM data acquisition layer.

This was achieved by combined use of the stream processing and of the batch processing features of the SIEM, which enabled the tool to spot deviations of observed values from past and/or typical values, which were not acceptable.

In the second attack scenario the indicator of compromise considered by the SIEM system to perform detection is composed of the values of the parameters being specified in the treatment plan. The output of TPS includes different files. They contain an output dose map and a radiotherapy plan. Since the files contain textual information regarding the plan and critical data that allow for LINAC setting and dose controlling, an attack to the integrity of data stored in these files could have dramatic consequences to the patient' safety. To protect these sensitive data from cyberattacks, Homomorphic Encryption is exploited. Based on context and historical information provided by external data feeds, the SIEM system performs analytics on the encrypted data by using comparison operators to verify whether the values of the proposed treatment plan are in the expected range for the specific cancer treatment.

Experiments demonstrated that the SIEM can detect the attacks in a timely fashion, i.e., with a response time which satisfies the requirements of the business process with a wide margin of safety. More precisely, the total duration of the business process (under the assumption of non-stop operation, i.e., without considering delays due to interactions with a human operator) is 30 min or more (depending on the data size of the specific study) while the response time (i.e., the detection latency) of the SIEM ranged from 1 to 5 min.

Related Work

An overview of related research is provided in "Enabling Technologies" (specifically, subsections "Homomorphic Encryption", "Trusted Execution Environment", and

Table 1 Solutions comparison

	TCO	Lifecycle support				Reuse of legacy	Distributed integrity check
		Plan	Do	Check	Act		
Commercial SIEM solutions	Medium to high	Low	High	Partial	High	High	Software
Commercial risk analysis solutions	Low to medium	High	Low	Medium	Low	High	N/A
Lightweight security solutions	Low to medium	Low or medium	High	Low	High	Medium	None or software
Our solution	Low	Medium	High	High	High	High	Software and hardware

"Open Source And COTS Software"). This section complements the treatment of related research with a brief yet right to the point analysis of the State of the Art of Risk Assessment and SIEM technologies.

Mainstream solutions for risk assessment (such as RSA[31], Rsam [32], MetricStream [33], OpenPages [34], RiskIQ [35] or FireCompass [36]) also cover cyber risks, but are typically hard to sustain for Smart Hospitals mainly because of their TCO (Total Cost of Ownership), and because of the limited usage with respect to the whole set of functionalities offered in the pricing plans. Smart Hospitals are then turning to lighter and more tailored solutions (such as: ThreatSketch [37] and GCA cyber Toolkit [38] that usually can be acquired and maintained at a lower cost. Both categories of solutions still have a knowledge barrier to be effectively adopted, that is mainly due to the lack of guidance in configuration and maintenance activities, from one hand, and in the indication of specific countermeasures that each Smart Hospital should adopt based on a cost/effectiveness evaluation of alternatives available on the market.

SIEM products have been reported and classified in Gartner's Magic Quadrant for SIEM solutions [39]. Gartner's research compares many products and classifies seven of them as leaders, which are: IBM, DELL, Exabeam, McAfee, Securonix, Splunk and LogRythm. Two promising building blocks of a security monitoring facility, which are not being exploited by currently available SIEM and security monitoring solutions in general, are Business Process Management (BPM) [40, 41] and Business Activity Monitoring (BAM) [42]. The current situation of the BPM market is reported in Gartner Magic Quadrant for Intelligent Business Process Management Suites [43]. In their January 2019 issue, Gartner evaluates many BPM suites recognizing as leader vendors the Pega, IBM, and Appian platforms. BAM is software that aids in monitoring of business activities, as those activities are implemented in computer systems. It provides near real-time monitoring of business activities, measurement of Key Performance Indicators (KPIs), their presentation in dashboards, and automatic and proactive notification in case of deviations. While it is arguable whether BPM and BAM enable organizations to be more efficient, more effective, and more capable of change, they surely process a whole lot of information that is related—sometimes quite closely indeed—to security.

A summary of reported solutions is presented in following table (Table 1).

Summary and Conclusions

This paper presented a risk assessment approach and an accompanying SIEM tool for improving the security of Smart Hospitals.

By relying on continuous monitoring of security relevant events, the risk-containment approach supports Smart Hospitals in understanding the risks they are up against and in prioritizing them based on detailed context information. This results in an increased level of security across valuable assets as well as with respect to data exchange. It further supports Smart Hospitals in the management of the residual risk, by enabling them to estimate it and thus to negotiate with insurance companies additional coverage for it.

The work presented in this paper builds on previous research done in the KONFIDO project. More precisely, the solution proposed in this paper relies on the same core technology developed in KONFIDO, which is customized via detailed modelling of the Business Processes that are to be protected. This allows the SIEM to timely spot behavioural deviations which might well result in major impacts.

We explicitly emphasize that the proposed approach favours compliance with current and upcoming regulations, and in particular: the Medical Devices Directive 93/42/EEC; the General Data Protection Regulation (GDPR) 2016/679; the Privacy and Electronic Communications Directive 2002/58/EC and the upcoming regulation foreseen for implementation in 2019; and the Cross-border HC Directive 2011/24/EU; all of which confer several articles on data protection and security.

In general, the proposed approach and accompanying SIEM tool favour the implementation of a continuous process towards cyber security improvement, since they help Smart Hospitals to achieve the following objectives.

1. Reduce the risk of malicious actions caused by cyberattacks (i.e., make Smart Hospitals safer).

2. Reduce the risk of data breaches (i.e., to improve the privacy guarantees given to citizens).
3. Empower Smart Hospitals to become the main actors of their cyber-resilience improvement process, by increasing personnel awareness and skills.
4. Support and encourage Smart Hospitals to take a comprehensive approach to risk management by defining the target level of risk and transfer residual risks to insurance providers.

In particular, the risk assessment phase enables the Chief Security Officer (CSO) of the hospital to identify the most critical business processes, i.e., those where a security breach may result in major impacts on patients' health (or even result in death). Critical business processes are then monitored by means of a customized Security Information Event and Management (SIEM) solution, i.e., which has been specifically tailored to the needs of hospitals and health care institutions. The SIEM provides advanced data processing and event correlation capabilities, which enable timely and accurate information about cyber-attacks, as well as directions for countering them and actions for mitigating their effects.

The proposed SIEM advances the state of the art of the technology, since it relies on the joint use of Homomorphic Encryption (HE) and Trusted Execution Environment (TEE) technologies to perform privacy preserving security monitoring. It allows a customer to trust third-party entities, because sensitive data will never be decrypted throughout its lifecycle, namely: creation, exchange, processing, and storage. The solution is low-cost and easy to install and maintain, and thus affordable even for Smart Hospitals of a relatively small size. This has been achieved by: (1) building on a selection of best of breed Open-Source products and tools, and (2) providing the possibility of deploying the SIEM solution on the cloud. The proposed approach can be applied both to active (i.e. which perform actions on patients) and to passive (i.e. which simply monitor patients) medical devices, both large (e.g., radiotherapy and imagery) and small (wearable devices and sensors).

To protect previous investments, the SIEM interoperates with market solutions from major vendors (that might have already been installed).

The approach was presented and validated with respect to a real use case, with challenging security requirements (deriving from critical safety issues). The use case was contributed by one of the major public hospitals of a European country. A fully functional implementation of the SIEM tool is already available, and the paper presented the main technical details, including the technologies that have been selected. Experiments demonstrated that the proposed risk assessment approach and associated SIEM tool can effectively improve the security of Smart Hospitals, since they support a technically sound management approach and provide protection mechanisms against cyberattacks which can have major impacts on the most critical asset categories of Smart Hospitals.

Funding Open access funding provided by Università Parthenope di Napoli within the CRUI-CARE Agreement. This study was funded by the European Union's Horizon 2020 research and innovation programme under Grant agreement No. 952179 INCISIVE (A multimodal AI-based toolbox and an interoperable health imaging repository for the empowerment of imaging analysis related to the diagnosis, prediction, and follow-up of cancer). This paper reflects only the authors' views, and the Community is not liable for any use that may be made of the information contained therein.

Declarations

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. Ponemon study on the Challenging state of vulnerability management. Balbix. (2020). Retrieved September 21, 2021, from https://www.balbix.com/press-releases/ponemon-report-on-vulnerability-management-challenges/.
2. Bindu Sundaresan. OSSIM. AT&T Cybersecurity. (n.d). Retrieved September 21, 2021, from https://www.alienvault.com/products/ossim.
3. Gartner I. Security information and event MANAGEMENT (SIEM Tools) Reviews 2021: Gartner peer insights. Gartner (n.d.). Retrieved September 21, 2021, from https://www.gartner.com/reviews/market/security-information-event-management.
4. IBM QRadar SIEM - Overview. IBM. (n.d.). Retrieved September 21, 2021, from https://www.ibm.com/products/qradar-siem.
5. Cyber security and resilience for SMART HOSPITALS. ENISA. (2021). Retrieved September 21, 2021, from https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals.
6. Mayra Rosario Fuentes, Numaan Huq. Challenges in SECURING CONNECTED HOSPITALS. (2018). Retrieved September 21, 2021, from https://www.trendmicro.com/en_us/research/18/d/challenges-in-securing-connected-hospitals.html.
7. Coppolino L, Dantonio S, Romano L, Sgaglione L, Magliulo M, Pacelli R. Protecting critical business processes of Smart Hospitals from cyber attacks. Proc 2019 15th Int Conf Signal-Image

Technol Internet-Based Syst SITIS. 2019. https://doi.org/10.1109/SITIS.2019.00065.
8. Report on Improving Cybersecurity in the Health Care Industry - Health Care Industry Cybersecurity Task Force. U.S. Department of Health and Human Services (2017). Retrieved September 21, 2021, from http://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
9. Staffa M, Coppolino L, Sgaglione L, Gelenbe E, Komnios I, Grivas E, Stan O, Castaldo L. KONFIDO: an OpenNCP-based secure eHealth data exchange system. In: Proceeding of Euro-CYBERSEC (2018).
10. Gentry C. Fully homomorphic encryption using ideal lattices. In: Proceedings of the forty-first annual ACM symposium on theory of computing ser. STOC'09, pp 169–78. 2009.
11. Naehrig M, Lauter K, Vaikuntanathan V. Can homomorphic encryption be practical? Proc 3rd ACM Workshop Cloud Comput Security Workshop CCSW'11 ACM NY USA. 2011. https://doi.org/10.1145/2046660.2046682.
12. Chen H, Gilad-Bachrach R, Han K, Huang Z, Jalali A, Laine K, et al. Logistic regression over encrypted data from fully homomorphic encryption. BMC Med Genom. 2018;11(4):81.
13. Microsoft. Microsoft/SEAL: Microsoft seal is an easy-to-use and powerful homomorphic encryption library. GitHub. (n.d). Retrieved September 21, 2021, from https://github.com/Microsoft/SEAL.
14. Brakerski Z, Gentry C, Vaikuntanathan V. Fully homomorphic encryption without bootstrapping. Electron Colloquium Comput Complex. 2011;18:111.
15. Chillotti I, Gama N, Georgieva M, Izabachène M. TFHE: fast fully homomorphic encryption over the torus. J Cryptology 2019;33:34–91.
16. Coppolino L, D'Antonio S, Formicola V, Mazzeo G, Romano L. VISE: combining intel SGX and homomorphic encryption for cloud industrial control systems. IEEE Trans Comput. 2020. https://doi.org/10.1109/TC.2020.2995638.
17. McKeen F, Alexandrovich I, Berenzon A, Rozas CV, Shafi H, Shanbhogue V, Savagaonkar UR. Innovative instructions and software model for isolated execution. Proc 2nd Int Workshop Hardw Arch Support Security Privacy HASP'13 ACM NY USA. 2013. https://doi.org/10.1145/2487726.2488368.
18. Costan V, Devadas S. Intel sgx explained. Cryptology ePrint Archive, Report 2016/086. (2016). http://eprint.iacr.org/2016/086.
19. Maene P, Gtzfried J, de Clercq R, Mller T, Freiling F, Verbauwhede I. Hardware-based trusted computing architectures for isolation and attestation. IEEE Trans Comput. 2018;67(3):361–74. https://doi.org/10.1109/TC.2017.2647955.
20. Zhao C, Saifuding D, Tian H, Zhang Y, Xing C. On the performance of intel sgx. 2016 13th Web Inf Syst Appl Conf WISA. 2016. https://doi.org/10.1109/WISA.2016.45.
21. Stateful computations over data streams. Apache Flink. (n.d.). Retrieved September 21, 2021, from https://flink.apache.org/.
22. Apache storm. Apache Storm. (n.d.). Retrieved September 21, 2021, from https://storm.apache.org/.
23. Esper. EsperTech. (2020). Retrieved September 21, 2021, from https://www.espertech.com/esper/.
24. Elastic stack: Elasticsearch, KIBANA, Beats & logstash. Elastic. (n.d.). Retrieved September 21, 2021, from https://www.elastic.co/elastic-stack.
25. Java native interface. JNI APIs and Developer Guides. (n.d.). Retrieved September 21, 2021, from https://docs.oracle.com/javase/8/docs/technotes/guides/jni/.
26. We enable secure execution of containers and programs using Intel SGX. SCONE - A Secure Container Environment. (n.d.). Retrieved September 21, 2021, from https://scontain.com/index.html?lang=en.
27. Graphene. (n.d.). Retrieved September 21, 2021, from https://grapheneproject.io/.
28. Apache Kafka. (n.d.). Retrieved September 21, 2021, from https://kafka.apache.org/.
29. Activemq. ActiveMQ. (n.d.). Retrieved September 21, 2021, from http://activemq.apache.org/.
30. Naehrig M, Lauter K, Vaikuntanathan V. Can homomorphic encryption be practical? In: Proceedings of the 3rd ACM workshop on cloud computing security workshop, ser. CCSW'11. New York, NY, USA, ACM, pp 113–24. 2011.
31. RSA cybersecurity and Digital risk management solutions. RSA.com. (2021). Retrieved September 21, 2021, from https://www.rsa.com/.
32. GRC software for Risk, compliance, and audit. Galvanize. (n.d.). Retrieved September 21, 2021, from https://www.rsam.com/.
33. Governance, risk and COMPLIANCE (GRC), CyberSecurity Solutions. Metricstream. (n.d.). Retrieved September 21, 2021, from https://www.metricstream.com/.
34. IBM openpages with Watson - Overview. IBM. (n.d.). Retrieved September 21, 2021, from https://www.ibm.com/us-en/marketplace/openpages-operational-risk-managemen.
35. Riskiq. RiskIQ. (n.d.). Retrieved September 21, 2021, from https://www.riskiq.com/.
36. FireCompass. (2021). Retrieved September 21, 2021, from https://www.firecompass.com/.
37. Threat sketch. Threat Sketch. (2020). Retrieved September 21, 2021, from https://threatsketch.com/solutions/.
38. GCA Cyber Toolkit. You are being redirected. (n.d.). Retrieved September 21, 2021, from https://gcatoolkit.org/smallbusiness/.
39. Gartner_Inc. Magic quadrant for security information and event management. Gartner. (n.d.). Retrieved September 21, 2021, from https://www.gartner.com/en/documents/3894573/magic-quadrant-for-security-information-and-event-manage.
40. TIBCO® BPM ENTERPRISE. TIBCO Software Inc. (n.d.). Retrieved September 21, 2021, from https://www.tibco.com/products/business-process-management.
41. Pega platform. Pega. (2020). Retrieved September 21, 2021, from https://www.pega.com/it/products/pega-platform.
42. Oracle Business Activity Monitoring. Oracle business activity monitoring. (n.d.). Retrieved September 21, 2021, from https://www.oracle.com/technetwork/middleware/bam/overview/index.html.
43. Gartner_Inc. Magic quadrant for intelligent business process management suites. Gartner. (n.d.). Retrieved September 21, 2021, from https://www.gartner.com/en/documents/3899484/magic-quadrant-for-intelligent-business-process-manageme.