SAFECARE

Integrated cyber-physical security for health services

Specification of e-Health Device Security Analytics

Deliverable 5.7

Lead Author: PEN

Contributors: PEN, PMS, CCS, CNAM

Deliverable classification: PU

Co-funded by the Horizon 2020 Framework Programme of the European Union

Version Control Sheet

Title	*Specification of the E-health devices security analytics [M12]*
Prepared By	*Brinda Hampiholi, Paul Koster*
Approved By	
Version Number	*1.0*
Contact	

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
V.01	02.07.2019	Initial draft for ToC and content	BH	
V0.2	23.07.2019	Adding new content to all sections	BH	
V0.3	06.08.2019	Third draft with updated content – Under internal review	BH, PK	
V0.4	16.08.2019	V4 is the working version as of 16-08-2019.	BH, PK	
V0.5	19.08.2019	Version V5 with feedback from PK and RV incorporated.	BH, PK, RV	
V0.6	22.08.2019	Version for SAFECARE review	BH, PK	
V1.0	29.08.2019	Final version. Review feedback from EOS, AMC and CNAM processed.	BH, PK	

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 787002.

Contents

LIST OF FIGURES

LIST OF TABLES

Table of Acronyms

Acronyms	Description
CIS	Clinical Information Systems
CT	Computerized Tomography
CVE	Common Vulnerabilities and Exposures
DICOM	Digital Imaging and Communications
DoS	Denial of Service
ICT	Information and Communications Technology
IDS	Intrusion Detection System
IoT	Internet of Things
IPSec	IP Security
MRI	Magnetic Resonance Imaging
NTP	Network Time Protocol
OS	Operating System
PACS	Picture Archiving and Communication System
PII	Personally Identifying Information
RIS	Radiology Information Systems
SOC	Security Operations Center
SSH	Secure Shell
TLS	Transport Layer Security
USB	Universal Serial Bus

Executive Summary

The challenge of SAFECARE is to bring together the most advanced technologies from the physical and cyber security spheres to achieve a global optimum for systemic security and for the management of combined cyber and physical threats and incidents, their interconnections and potential cascading effects. The project focuses on health service infrastructures and works towards the creation of a comprehensive protection system, which will cover threat prevention, detection, response and, in case of failure, mitigation of impacts across infrastructures, populations and environment.

Over a 36-month timeframe, the SAFECARE Consortium will design, test, validate and demonstrate 13 innovative elements, developed in the Document of Actions, which will optimize the protection of critical infrastructures under operational conditions. These elements are interactive, cooperative and complementary, aiming at maximizing the potential use of each individual element. The consortium will also engage with leading hospitals, national public health agencies and security Stakeholders across Europe to ensure that SAFECARE's global solution is flexible, scalable and adaptable to the operational needs of various hospitals across Europe, and meet the requirements of newly emerging technologies and standards.

This deliverable (D5.7) specifies the E-health devices security analytics solution. This cybersecurity solution provides security monitoring and analytics for medical devices. Its results feed into threat and incident management workflows, product support workflows and security risk management models and processes. The first ensures that incidents or vulnerabilities are resolved by hospital, security provider or medical device manufacturer. The latter ensures that insights are taken into account in the product research and development process.

The specification describes the architecture of the solution to be realized and demonstrated in SAFECARE context. It covers the security analytics tool, the end-to-end infrastructure and the security analytics models. This is driven by requirements and scenarios presented in this document.

In a nutshell, the E-health device security analytics solution architecture focusses on acquiring, monitoring and analyzing medical device log data to detect security events and other security relevant data. It generates alerts when events or vulnerabilities are detected and sends alerts to the relevant stakeholders' systems.

Early experiments with the incomplete infrastructure and available medical device log data demonstrate that E-health device security analytics is a practical and effective approach. The results are useful for security monitoring, threat detection and reporting.

The next step will be the realization of the specification and delivering the E-health devices security analytics prototype (Deliverable D5.8).

The SAFECARE Project

Over the last decade, the European Union has faced numerous threats that quickly increased in their magnitude, changing the lives, the habits and the fears of hundreds of millions of citizens. The sources of these threats have been heterogeneous, as well as weapons to impact the population. As Europeans, we know now that we must increase our awareness against these attacks that can strike the places we rely upon the most and destabilize our institutions remotely. Today, the lines between physical and cyber worlds are increasingly blurred. Nearly everything is connected to the Internet and if not, physical intrusion might rub out the barriers. Threats cannot be analyzed solely as physical or cyber, and therefore it is critical to develop an integrated approach in order to fight against such combination of threats. Health services are at the same time among the most critical infrastructures and the most vulnerable ones.

They are widely relying on information systems to optimize organization and costs, whereas ethics and privacy constraints severely restrict security controls and thus increase vulnerability. The aim of this proposal is to provide solutions that will improve physical and cyber security in a seamless and cost-effective way. It will promote new technologies and novel approaches to enhance threat prevention, threat detection, incident response and mitigation of impacts. The project will also participate in increasing the compliance between security solutions and European regulations about ethics and privacy for health services. Finally, project pilots will take place in the hospitals of Marseille, Turin and Amsterdam, involving security and health practitioners, in order to simulate attack scenarios in near-real conditions. These pilot sites will serve as reference examples to disseminate the results and find customers across Europe.

1 Introduction

The healthcare sector has been facing an increasing cybersecurity risk over the last few years. This can be attributed to increasing connectivity of medical devices to computer networks and convergence of technologies in the healthcare sector that has exposed vulnerable devices and software applications to security attacks. The attacks need not be only focused on compromising patient data, but it may also be about compromising the medical devices within hospitals. The attacks that target medical devices are far more concerning as they have potential impact on clinical care and safety of humans involved. For instance, a device infected with malware has the potential to disrupt hospital operations, expose sensitive patient information, compromise other connected devices, and harm patients. In another instance, a compromised X-ray device could cause radiation overdose or uncontrolled movement of mechanical parts thus physically harming not only the patients but also clinical staff in the vicinity of the device. Therefore, ensuring medical device security is crucial for any healthcare organization.

Medical device security impacts device and human safety. Security requirements have increased over time and they need to be taken into account during device design and development. To ensure medical device security, it is necessary to better apprehend potential risks, detect security events as soon as possible and plan mitigation measures. This follows recommendations like FDA post-market guidelines[1] and continuous security monitoring to realize risk identification and detection capability from NIST's cybersecurity framework[2].

Ensuring security of medical devices is a joint responsibility of medical device manufacturers and their customers, i.e. healthcare providers[3]. The manufacturers need to apply security by design approach to design and development of the devices and provide configurable security features on the devices that their customers can configure based on the environment in which the devices are deployed. They also have the potential to provide security monitoring services to help their customers maintain adequate level of security thus reducing risks. The healthcare providers need to use appropriate technical, physical, and procedural means to maintain a secure environment in which the devices will operate. Insufficient maintenance may leave operational issues undetected and unresolved, both in terms of cybersecurity posture, but also in terms of patient care operations. Therefore, ensuring security in healthcare infrastructures requires collaborative efforts among the stakeholders.

The SAFECARE project aims at achieving security solutions in healthcare infrastructures through collaboration among the stakeholders. One such cybersecurity solution is "e-Health device security analytics". This solution is a practical and effective approach to security monitoring, threat detection and reporting. It aims at reducing cybersecurity risk stemming from medical

[1] **FDA. 2016.** *Postmarket Management of Cybersecurity in Medical Devices - Final Guidance.* 2016.

[2] **NIST. 2014.** *Security Controls and Assessment Procedures for Federal Information Systems and Organizations.* 2014. NIST SP800-53 (Rev.4).

[3] **ISO. 2016.** *IEC 80001-2-8:2016(en) Application of risk management for IT-networks incorporating medical devices.* s.l. : ISO, 2016. IEC 80001-2-8:2016.

devices that have been deployed at healthcare providers' sites and improving the overall security of the medical device infrastructures.

1.1 Purpose and scope

The current document is Deliverable 5.7, one of the deliverables within Work Package 5 in the SAFECARE project. It provides the description and design specification of E-health device security analytics solution. This solution collects data from medical devices, performs analytics to derive meaningful security data, and makes it available in normal form for further use. Hereby, it aims at contributing to improve product security risk assessment and management of connected e-health devices. Specifically, it targets to strengthen the quantitative and/or model-based approach to security risk assessment and management by creating actionable security insights.

The analytics combines data from the installed base and other (public) data sources. It will apply data mining, machine learning and deep learning techniques on the available data to identify potential security events, risks and threats to medical devices in their environment.

The security analytics solution will utilize the existing support infrastructure such as device logs and complaint management systems to identify meaningful security attributes and risk indicators. Examples include device software configuration, installed patches and authentication sessions.

Given that medical devices today are typically not yet instrumented to act as a key source of security data, the security analytics solution will propose extensions to improve this. E-health devices in scope concern radiology equipment, which may be generalized to include automated syringe, any electronic equipment fixed on the patient catheter, scanners, and medical database.

1.2 Definitions

Term	**Description**
Alert	Notification that a specific attack has been directed at an organization's information systems.
Attack	An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity, availability, or confidentiality.
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Security risk	The level of impact on agency operations (including mission functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
Threat event	An event or situation that has the potential for causing undesirable consequences or impact.

Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Table 1 Security term definitions according to NIST glossary[4]*.*

1.3 Methodology

This deliverable document was prepared using a combination of desktop research, system architecting and design, and experiments done on the logs generated by medical devices to detect security events. The methodology followed in this document is as follows:

1. Describe a typical medical device setup that consists of advanced radiology equipment, enumerate security threats to such medical devices and present some example scenarios.
2. Perform a requirement analysis and state the requirements for an e-health device security solution.
3. Describe the solution: e-health device security analytics, the specifications and the system architecture.
4. Perform experimental security analytics.

[4] https://csrc.nist.gov/glossary/

2 Medical device security

Medical devices are increasingly connected to the Internet, hospital networks, and other medical devices to enable health care providers to provide better health care to the patients. The benefits of such advanced devices include improved diagnostics, enhanced surgical ability, seamless patient flow, and remote medical care among others. However, hyper-connectivity and advanced ICT features of the medical devices also increase the risk of potential cybersecurity threats. Medical devices, like other computer systems, can be vulnerable to security breaches, potentially impacting the safety and effectiveness of the device.

In this section, an example medical device setup is described to provide an idea of the setup in which medical devices are important assets and ensuring security of such devices is extremely important. This setup description is followed by the list of potential security threats that are prevalent in such medical device environments. Then some example attack scenarios are discussed where security analytics can be very useful in attack detection and response planning.

2.1 Medical device setup

The security analytics solution under consideration is generic for medical devices that operate in a healthcare environment. However, to support its development, we select a representative class of medical devices and focus here on diagnostic medical devices such as radiology equipment (X-ray devices, CT scanners). Henceforth, they are referred as ‘devices’ in the document. An example infrastructure in which these devices are found is given in Figure 1 and Figure 2.

The physical setup consists of devices that have been manufactured by device manufacturers and then deployed at hospitals. These devices are operated from within the hospital by the hospital staff. Maintenance of these devices is done locally at the hospital or remotely by the manufacturer’s staff (e.g. field service engineers or remote service engineers).

Device manufacturer is responsible for (i) device development and testing before the device is licensed and deployed at the customer hospital and (ii) device maintenance and log retrieval during the time it is operable inside the hospital. Log retrieval and aggregation is periodically conducted by the manufacturer. The device manufacturer needs the log data for providing device maintenance and other remote services to the customer hospital. This data is also useful for product improvement purpose.

In the example setup, the devices are placed in an examination room where the patient is examined. The device is connected to a multi-screen display, the computers in the control room and to the computer cluster in the technical room. Details of how the device setup is distributed in the afore-mentioned locations are given below.

Examination room: The patient lays down on the device and the examination is performed. The doctor can view the patient’s personal data, medical history and results from the current examination on the multi-screen display.

Control room: A clinician is responsible for creating new patient records or pulling up the medical records of the patient who is currently being examined in the Examination room, on one of the computers in the control room.

Technical room: This room hosts the computer cluster that collects all the patient data (personal data, medical visit history and images resulting from the examination) from the devices in the examination room. The device and the computers in the control room are connected to this computer cluster.

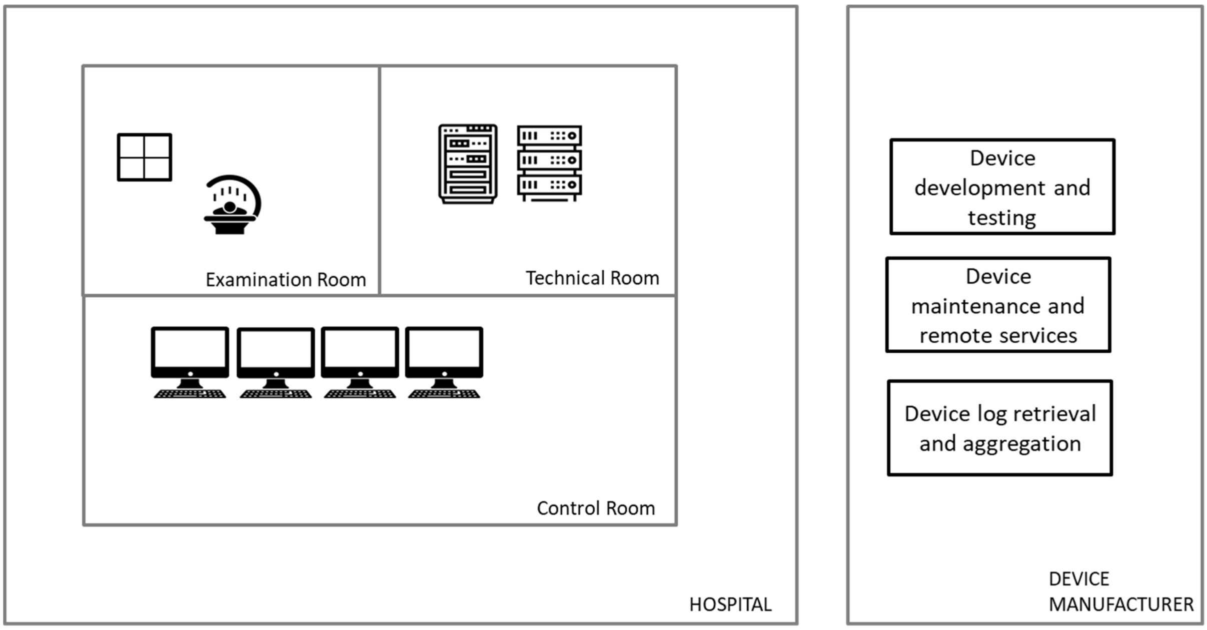

Examination Room
Technical Room
Control Room
HOSPITAL
Device development and testing
Device maintenance and remote services
Device log retrieval and aggregation
DEVICE MANUFACTURER

Figure 1 Example medical device hardware setup

From a connectivity/networking view, the X-ray modality has multiple external interfaces used by other medical devices and vice versa as depicted in Figure 3. In addition, the X-ray modality uses services hosted within the hospital environment and at the device manufacturer.

Intervention Room: Combination of the examination, control and technical room. Within this area a number of protocols are used between the X-ray modality and adjacent 3rd party systems:

- Industry standard (transport) protocols e.g. https, IPSec, NTP, and DICOM are used for various use cases such as exchange of medical data, remote service and time synchronization.
- Depending on the level of integration proprietary protocols might be used to communicate additional data and/or to control the other system.
- Several security mitigations including preconfigured firewalls are used to limit exposure of these protocols to the intended system(s) and thus prevent exposure on the hospital network.

Hospital: System in the intervention room including the X-ray modality use IT services on the hospital network for normal system operation. Some examples:

- Patient demographics is exchanged with Radiology Information Systems (RIS) or Clinical Information Systems (CIS)
- Medical data is pushed by the X-ray modality to a central Picture Archiving and Communication System (PACS) at examination closure using DICOM protocol. If needed the physician can also query the PACS system for previously obtained (CT, MR or other modality type) examination results from a patient. DICOM is an unencrypted protocol which can be encrypted if both involved parties support secure DICOM.
- Any interaction with the system and related data is logged and systems can be configured to send audit-trail messages to customer syslog systems.

Device Manufacturer: built remote service capabilities into products to guarantee maximum uptime or optimize hospital workflow by:

- Proactively monitoring of device/component health status via device log files obtained over *https* based tunnel.
- Re-active service functionality via *https* based tunnel to change settings or update software.

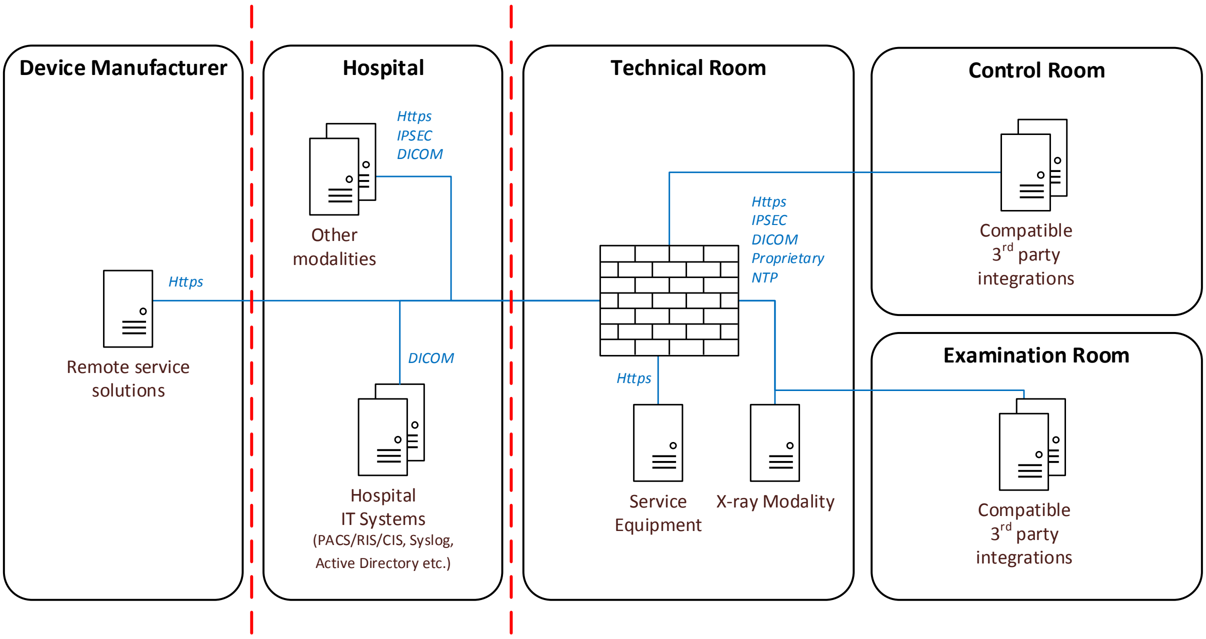


Figure 2 Example medical device connectivity setup

2.2 Security threats to medical devices

This section provides a summary of prevalent threats that can affect medical devices and in turn have consequences for hospitals, patients, device manufacturers etc. This list of threats is taken from the ENISA report[5] and has been filtered and adapted in the current context of medical device security.

Threat types:

- Malware: Malware is a major threat to critical infrastructures such as healthcare because it can infect a great number of end devices. The multitude and heterogeneity of such devices in a hospital (e.g. stationary medical devices, computers, mobile devices and wearable devices) result in a particularly large attack surface. In terms of specific malware concerns, ransomware has been identified as a major threat for healthcare organizations. Other categories of malware include worms, viruses, Trojans, spyware, rootkits, botnets etc.
- Hijacking: Hijacking may be performed at network level or at device level. In the healthcare infrastructure context, device hijacking is more significant. TrapX Security introduced the term "Medjack" to refer to the hijacking of medical devices to create backdoors in hospital networks.

[5] **ENISA. 2016.** *Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures.* 2016.

- Device tampering: Networked medical devices may be reprogrammed, reconfigured by changing device settings or deactivated. This poses a major threat to the security of the healthcare system but also to patient safety. If a tampered device malfunctions during a patient examination, then it may cause faulty diagnosis, treatment and potential harm to the patient. Furthermore, tampered devices may adversely affect the cybersecurity posture of the entire healthcare system.
- Device and data theft: Device theft may be a rare physical security attack when considering the volume some of the medical equipment. However, when introducing sensors, volume is not an issue anymore and the likelihood of this attack to be realized increases. Not having all the interconnected devices in place might lead to wrong data collection, wrong analysis thus wrong decision making.
- Denial-of-service attacks: Such attacks might render a medical device or service altogether unavailable, which could potentially fully disrupt a patient care process. As medical devices are increasingly connected to many computer systems and rely on web or cloud resources, a DoS attack might, for instance, result in unavailability of patient data (e.g. if data is stored in a cloud environment or if their collection is Internet-based for remote patient care purposes).
- Human errors leading to absence of audit logs to allow for appropriate control - e.g. for incident identification and assessment of corrective/improvement actions.
- Unauthorized access to medical device: This attack may lead to device tampering, compromise of patients' confidential data, disruption in device operations etc. Such an attack is highly pertinent to medical devices particularly due to the sensitivity of patient data involved and due to the criticality of the medical processes in which the devices are used.
- Software failures: These failures impact or completely disrupt a medical (e.g. failure of a PACS) or administrative process (e.g. patient data availability compromised). Such events must be prevented or at least detected quickly and resolved.

Threat actors:

- Insiders: These are hospital staff (any role) with malicious intent. This could be physicians, nurses, administrative staff, or even patients and other guests at the hospital who have a malicious intent to harm the hospital assets such as medical devices, ICT systems, and its reputation.
- External attackers: These are individuals or entities which are not in the physical vicinity of the medical equipment but can take malicious actions to evade the security of the equipment. For instance, a security researcher who aims at exploiting and exposing security vulnerabilities or a hacker who is financially motivated.
- Other causes: Environmental or accidental equipment/software failure or even external maintenance staff can cause security incidents, yet have no active attacker.

2.3 Attack scenarios

This section describes two examples of attack scenarios that are prevalent and impactful in the context of medical device security. These examples give an idea of scenarios in which security analytics can play a definitive role. In critical healthcare infrastructure, analytics can help the stakeholders in detecting security incidents and responding to them. It also provides valuable inputs and insights to improve the risk management model of medical devices.

In the following example scenarios, a security analytics solution that is specialized for healthcare infrastructure will perform better than an off-the-shelf, general-purpose intrusion detection system or an antivirus. This is because security analytics includes domain knowledge and analyzes and learns from the medical devices and their environment. It can effectively identify certain specific suspicious device behavior as a potential malware attack or an attack due to unauthorized access. The scenarios in chapter 4 work this out further.

Attack scenario 1	
Type of attack	Malware or virus infection
Description	A malware infects a (or some) device(s) which can interfere with normal functioning the device or cause data exfiltration. This may endanger the safety of the patient or cause disruption to the medical treatment. If not contained, the malware may spread inside the device's network and infect other medical devices and systems. It may also cause financial loss due to downtime of the devices and reputation loss for the hospital as well as the device manufacturer.
Exploited vulnerability	Outdated antivirus versions running on the device, latest security patches from the manufacturer not installed on the device, unprotected interfaces such as USB that may allow easy entry of the virus/malware into the device network
Severity	High – The severity or criticality is high because of the broad range of follow-up attacks that may be possible. Medical devices in hospitals are increasingly connected with clinical and enterprise information systems. The key problem is that vulnerable devices are brought together with highly valuable data.
Likelihood	Medium – Medical devices have become easy and pivot points for attacks within healthcare context. The likelihood is medium as most of the medical devices include basic security features such as antivirus, intrusion detection mechanisms.
Mitigation plans	The measures that can be taken to mitigate the consequences of this attack or to prevent the attack in future are as follows. - Regularly monitor the status of antivirus and other security features on the medical devices. - Enable installation of latest security patches on medical devices. - Apply security controls such as not allowing USB drive insertion directly on medical devices or allowing them only after a thorough scan and cleanup of suspicious files on USB drives. - Monitor log activity to detect any suspicious behavior on the devices that follows an event such as a file transfer from a USB drive.

Attack scenario 2	
Type of attack	Unauthorized access and modification of device configuration data
Description	Illegal access and modification of device configuration data by an attacker may lead to malfunctioning or failing of the device. This may endanger the safety of the patient or cause disruption to the medical treatment. It may also cause financial loss due to downtime of the device and reputation loss for the hospital as well as the device manufacturer.
Exploited vulnerability	Weak baseline access control over device configuration files, unmonitored access and changes to device configuration over long time
Severity	High – The severity or criticality is high because of the broad range of follow-up attacks that may be possible. Medical devices in hospitals are increasingly connected with clinical and enterprise information systems. The key problem is that vulnerable devices are brought together with highly valuable data.
Likelihood	Medium – Medical devices have become easy and pivot points for attacks within healthcare context. The likelihood is medium as there are usually some access control in place in critical medical devices.
Mitigation plans	The measures that can be taken to mitigate the consequences of this attack or to prevent the attack in future are as follows. - Replace weak with strong access control mechanism - Regularly monitor configuration changes to detect the changes were legitimate or unauthorized.

3 Requirements

This section presents different types of requirements for the e-health device security analytics solution. The requirements mentioned in the SAFECARE requirement analysis deliverable D3.4 "Initial requirements analysis" that are relevant for medical device security are also integrated in this section.

3.1 Functional requirements

The main goal of security analytics solution is to utilize medical device log data to detect cyber-security risks across deployed medical devices and send timely alerts. The specific functional requirements for the solution are as follows.

- Security trend analysis: The solution should analyze logs from medical devices to detect trends that indicate potential security attacks such as malware infestation or data leakage.
- Anomaly and device misuse detection: The solution should be able to detect suspicious events from the logs, improper user account usage such as shared accounts, unauthorized access and data modification and other security events.
- Post-incident analysis: The solution should facilitate forensic investigations of security incidents.
- Alert generation: The solution should generate timely alerts for the detected security events and send them to relevant stakeholders.
- Input to risk management model: The solution should provide insights about the security posture of the devices and its environment that becomes input to the risk management model of the devices.
- Accuracy: The solution should be able to distinguish likely threats from normal usage with a reasonable degree of accuracy.
- Vulnerability detection: The solution should inform relevant stakeholders (e.g. operators) of passively detected system vulnerabilities, even if they are not being actively exploited. For example, the security analytics solution should detect and inform the operators if security functions on medical devices are not functioning (correctly) and if the devices have unpatched vulnerable components.
- Specialization: The solution should offer healthcare-specific specialized functionality over a general-purpose intrusion detection system (IDS) product.
- Learning: The solution should permit a learning approach from the impacts of real incidents that have occurred in the past.

3.2 Security and privacy requirements

Security and privacy requirements come from different sources including PIA, SAFECARE project and customer-vendor agreements. A privacy impact assessment is performed for the security analytics undertaking as documented in deliverable D3.9 "Analysis of ethics, privacy and confidentiality constraints". The solution should meet these requirements to ensure compliance with data protection laws. The objective of data processing in e-health medical device security analytics, type of data processed, security and privacy requirements are all detailed in this assessment. The SAFECARE security requirements provided in the requirements analysis deliverable D3.4 "Initial requirements analysis" are integrally considered in this design and specification of security analytics. A concise list of security and privacy requirements are provided below.

- Privacy by design and by default: The solution should process data in a way that complies with data minimization, purpose limiting, and limited data retention.
- De-identification: The solution should ensure that all the log and service data is de-identified (before leaving medical devices) so that no residual personal data is remaining before it is processed by the security analytics solution.
- Access control: The solution should take measures to prevent unauthorized access to the security analytics solution, for instance, by applying logical access control mechanisms.
- Malware resistance: Measures to clamp down malicious software from affecting security analytics should be put into place.
- Security training: Appropriate security training should be provided to the employees to access, use and interpret the results of security analytics.
- Operational security: The solution should not introduce new security vulnerabilities to medical devices or their environment that would not be present if the solution was not implemented.
- Safe failures: When the solution crashes or becomes unavailable for some reason, this should not affect the availability of the medical systems it is connected with. The damage should be limited to unavailability of security alerts.

3.3 Communication interface requirements

The external interface requirements depend on the input that the security analytics gets and the output that it generates and disseminates to relevant stakeholders. Figure 3 shows all the communication interfaces between the security analytics solution and other SAFECARE components. The blue arrows in the figure represent the internal communication interfaces and red arrows represent the external interfaces.

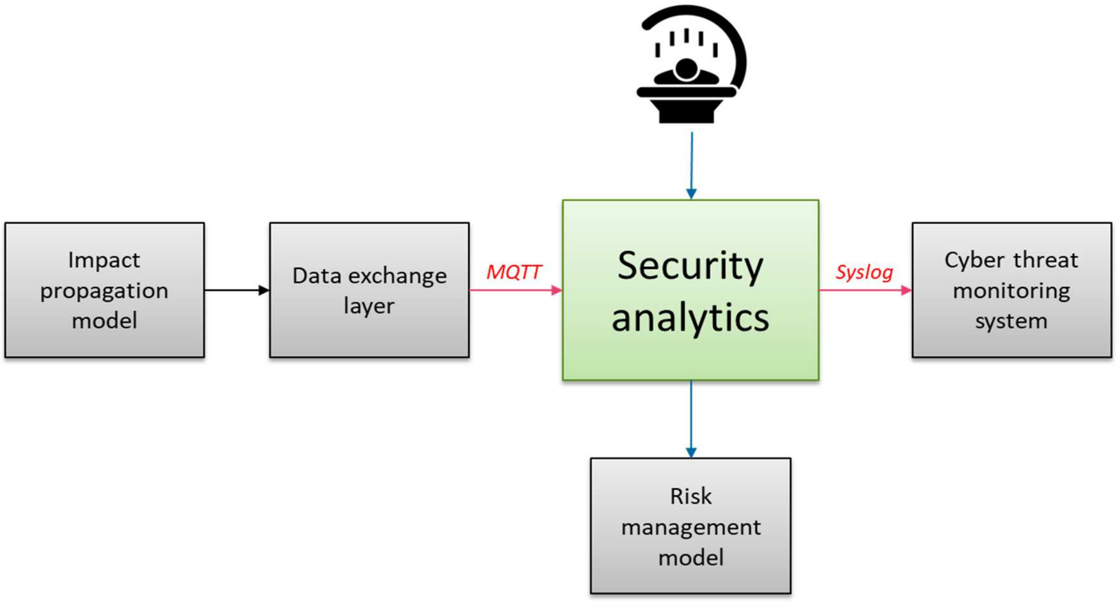


Figure 3 Communication interfaces

Internal interface requirements:

- Medical devices - Security analytics: The input to the solution is a collection of the device logs that come from the medical devices. It leverages the support infrastructure that collects the logs and aggregates them in a data warehouse.
- Security analytics - Risk management model: The output from the security analytics solution is a combination of security insights and event alerts. These are shared and used internally for the purpose of improving the risk management model for assessing security risk in medical devices and also to take appropriate actions based on the type of alerts.

External interface requirements:

- Data exchange layer - Security analytics: The security analytics solution may receive as input a list of impacts from an impact propagation module via data exchange layer. The communication protocol for this particular interaction is MQTT (Message Queuing Telemetry Transport)[6]. This interface should be supported by the security analytics solution.
  The interface and message formats will be specified in D6.2 "Specification about data exchange layer", D6.3 "Data exchange layer", D6.6 "Specification of the impact propagation and DS models" and D6.7 "Impact propagation and decision support model" respectively.
- Security analytics - Cyber threat monitoring system: The events and alerts need to be sent from the security analytics solution to the Cyber threat monitoring system using Syslog protocol[7]. The alert messages will be tunneled over TLS.
  The interface and message formats will be specified in D5.9 "Specification of the cyber threat monitoring system" and D5.10 "Cyber threat monitoring system" respectively.

3.4 Performance requirements

The requirements in terms of overall performance of the security analytics solution is as follows.

- Non-interference: Security analytics will not interfere with communication between, or the functionalities of, medical devices and other existing infrastructure, both in terms of CPU load and network traffic.
- Event detection time: Security analytics is not a real-time service. The device logs are sent from the medical devices stationed at the healthcare providers (e.g. hospitals) to the device manufacturer at predefined times. The security analytics solution runs within the device manufacturer environment. Event detection by the solution can be done only when the device log files are made available to the security analytics solution. This depends on the availability of the hospital network, remote service network of the device manufacturer etc. that is not under the control of the analytics solution. In the best case, events could be detected on average within 2 days, with 1 day being the target and not more than 5% exceeding 7 days. Non-critical events include e.g. baseline security configuration deviations, share requirements of non-security pro-active monitoring.

[6] https://docs.oasis-open.org/mqtt/mqtt/v5.0/mqtt-v5.0.pdf

[7] **IETF. 2009.** *The Syslog Protocol.* 2009. RFC 5424. Documentation available at https://solutions.ietf.org/html/rfc5424.

- Alert generation time: Events identified as critical should be immediately forwarded to responder or to SOC operators. Non-critical events should be reviewed within a day before forwarding to responder.
- Input to risk management model: The output of analytics solution such as events and security insights should be sent to the medical devices' risk management model on on-demand basis.

3.5 Other requirements

Some requirements that are not covered in the above sections are mentioned below. These requirements are inherited from the requirements provided by SAFECARE deliverable D3.4 "Initial requirements analysis".

- Security updates: When a new relevant vulnerability is published, the solution should receive an update that allows it to detect exploitation of this issue. There should be an easy and a resilient way to get the updates.
- Portability: The solution should not rely too much on the specifics of a deployment environment, such as a particular brand of firewall or router being in use, or operators using one type of operating system or browser.
- Customizability: Operators should be able to manually tweak the configuration to reduce the number of false positives/negatives. That is, the ones who get alerts should also be able to add some custom rules to the security analytics system.
- Scalability: The solution should be scalable across different groups of operators examining different types of events, scalable in different situation such as when the volume of log data increases.
- Traceability: Sufficient information should be provided in the generated alerts so that responders can identify an issue, and the actors involved with it.

4 Scenarios

This section presents some exemplary scenarios the e-health device security analytics functionality intends to support.

Figure 4 shows the clinical setup in which medical devices and the connected IT systems are found and provides annotations that make the data storage and access locations. The scenarios described in the following subsections can occur in such a clinical setup.

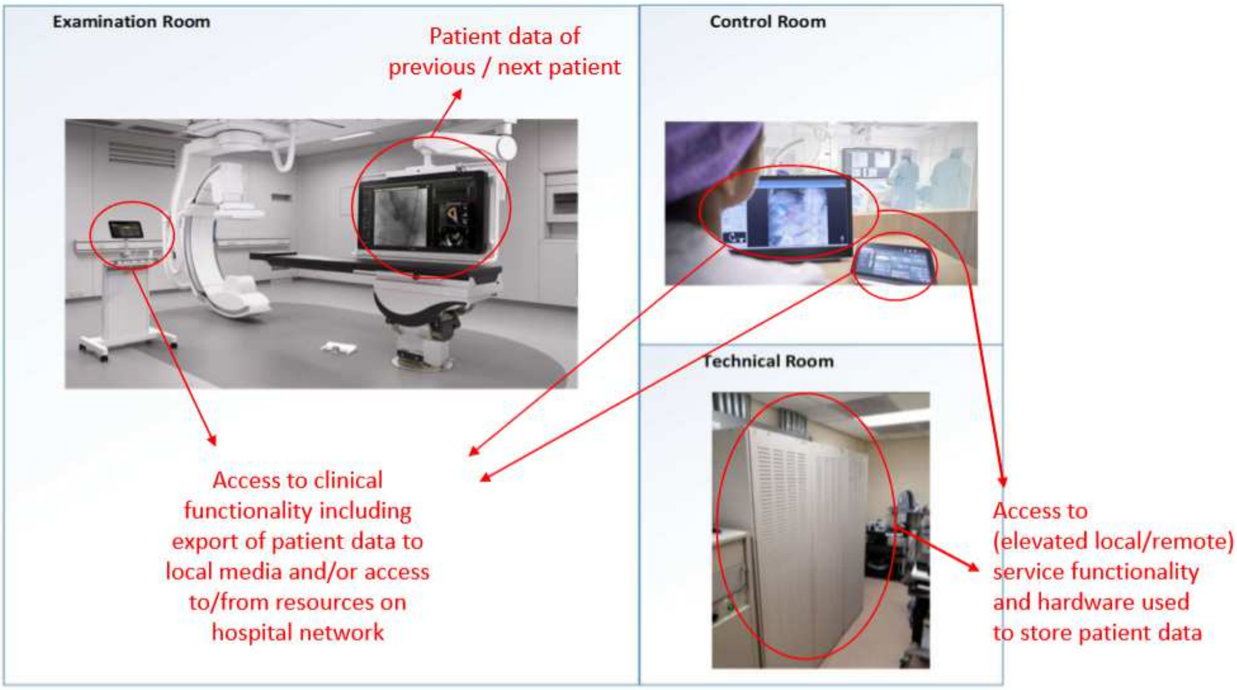

Examination Room
Patient data of previous / next patient
Control Room
Technical Room
Access to clinical functionality including export of patient data to local media and/or access to/from resources on hospital network
Access to (elevated local/remote) service functionality and hardware used to store patient data

Figure 4 Clinical setup diagram with annotations

The deliverable D3.6 provides a description of the relevant use-case scenarios which exploit combined physical and cyber threats in the healthcare sector and how they can impact and destabilize health services. This section will go through a subset of the scenarios in Deliverable D3.6 that are applicable to the medical devices and their cybersecurity and where the security analytics solution is appropriate to detect security events that resemble attacks. The scenarios are partly based on deliverable D3.6 "Definition of the cyber-physical scenarios of threat" extended with some further security monitoring and risk management scenarios.

4.1 Scenario 3: Cyber-physical attack targeting medical device infrastructure

Under Scenario 3, we consider the following technical scenarios.

4.1.1 Introduce a hardware fault in a medical device

The steps followed by an attacker in this attack scenario are as follows.

Step 1: An attacker uses social engineering or phishing to acquire a hospital staff's credentials to access the computer connected to the medical device.

Step 2: The attacker remotely connects and logs in to the computer by using the acquired credentials.

Step 3: The attacker alters the software on the medical device via the computer and cause a hardware fault in the device.

Here the security analytics solution can detect the hardware fault and trace the actions that led to this fault. It analyses the user login session in which the fault occurred and alert the hospital staff about the unauthorized access to the system in the control room and a possible compromise of the staff's credential. This will trigger further investigation within the hospital and help in finding the vulnerabilities in the system and environment that caused this event.

4.1.2 Device manufacturer impersonation

The steps followed by an attacker in this attack scenario are as follows.

Step 1: An attacker finds out all the information about the device, its manufacturer and the ways how manufacturer connects to the device remotely for maintenance or pushing updates.

Step 2: The attacker impersonates the manufacturer by exploiting a vulnerability in the hospital network and connects to the medical device

Step 3: The attacker installs a malicious software on the device. The software connects to a medical database from the device and encrypts/deletes/corrupts the database.

In this scenario, all the steps involve events that are logged by the device. From the logs, security analytics solution detects the following main events: an unknown IP address connecting to the medical device and a subsequent log in event, installation of a software on the device, possible configuration setting modifications, device's request to connect to patient database and modification of the database.

4.2 Scenario 6: Theft at hospital equipment, access to hospital network and IT systems

A technical scenario under Scenario 6 can materialize into an attack in the following steps. .

Step 1: An attacker gains access to the technical room by stealing the key or tricking a colleague into facilitating access to the room.

Step 2: Unplugs the hard drive that is in the technical room.

Step 3: The attacker accesses the contents of the hard drive, makes modifications or transfers all the contents to another hard drive and leaves the hospital with the stolen hard drive data.

As this scenario involves physically entering the technical room, getting hold of the hard drive and transferring all contents of the hard drive to his own storage device, all the physical actions are not logged. Physical security solutions presented in Deliverable 4.3 could be useful in detecting such physical security risks. However, the event that a disk gets unplugged result in errors that are logged by devices using that disk at that time. The security analytics solution could potentially process these logs and generate a useful alert that could later be correlated with physical events.

4.3 Scenario 7: Security in IoT medical devices

Some technical scenarios considered under Scenario 7 that target healthcare infrastructures indirectly by attacking devices and device manufacturers are given below.

4.3.1 Vulnerability Scanning

The steps taken by an attacker in this scenario are as follows.

Step 1: An attacker gets local access to a second-hand device or remote access to a device deployed in hospital.

Step 2: The attacker finds a vulnerability in the device by reverse engineering and plans to exploit it.

Step 3: The attacker exploits the vulnerability thereby causing disruptions to the operations at the hospitals where the devices are installed.

Here, the security analytics solution is looking for known vulnerabilities in medical devices that will create security threats. For instance, vulnerabilities can be the result of vulnerable software or insecure configurations. The security analytics solution can pick up on such vulnerable software versions and configurations. The manufacturer can fix the vulnerability and patch the deployed systems before an attacker learns about the presence of this vulnerability and exploits it.

4.3.2 Remotely attack devices connected to the public internet

An attacker may take the following steps to remotely connect and attack the medical devices that are connected to the public internet (i.e. accessible beyond the hospital's trusted network).

Step 1: An attacker finds out that a medical IoT device is accessible to public on the internet.

Step 2: The attacker remotely connects to the device and tries to log into the device. If the login is successful, then the attacker can compromise the security of the device and other connected systems in the hospital network. Some of the attacks include denial of service (DoS) attack where the attacker sends a large volume of data requests to the device, unauthorized file modification, installing a malicious software on the device.

Security analytics solution can continuously monitor application and firewall logs and analyze the access attempts made to a medical device from IP addresses outside the hospital's trusted network. If found, then it alerts the hospitals to tighten the network security and ensure that no devices are accessible via internet to entities outside the hospital network. Furthermore, it can register patterns of a DoS attack from the logs and provide insights to the manufacturer so that the risk management model of devices could be improved.

4.4 Other security monitoring and risk management scenarios

4.4.1 Security configuration deviation

Security configuration deviations are a typical prelude to security incidents later in time. For example, customers or support staff may turn off firewalls or antivirus for some reason and not re-enable them, leaving devices to operate out of their normal configuration and vulnerable. Ideally, this is addressed within some reasonable time as the risk grows with the time the device is left vulnerable.

In this scenario the security analytics solution notices from device logs that medical device security configuration deviates from the baseline without one of the regular (temporary) exceptions being applicable. Upon detection, an alert is generated which may trigger a case to be opened to resolve the situation by support staff.

The analytics solution will also generate aggregated statistics that will be sent as input on-demand to the risk management model which in combination with data on actual incidents improves the risk estimate. Subsequently, this is used in the R&D process to prioritize security mitigations in the most effective way.

4.4.2 Security function failure

Empirical research shows that endpoint security agents will fail almost by definition[8]. Examples are antivirus agents that no longer update their definition files, and software whitelisting solutions that fail to start their service.

In this scenario the security analytics solution notices from medical device logs that security agents fail to operate correctly. Upon detection, an alert is generated which may trigger a case to be opened to resolve the situation by support staff. Aggregated statistics also feed into the risk management model as presented in the previous scenario.

4.4.3 Security function usage

Presence of security features on medical devices does not imply it is used. Feedback on security function usage makes it possible to estimate risks more accurately, improve security functions to improve adoption, raise awareness, etc.

In this scenario, the security analytics solution detects if optional security features are used by a medical device. Detecting that personal authentication is not used or is used in unintended manner can feed into the risk management process to update the risk and improve in the next product version.

[8] https://www.absolute.com/go/study/2019-endpoint-security-trends

5 System design architecture

This section describes the architecture of the security analytics solution for security monitoring and analytics of medical devices and their environment. The solution acquires and analyses the security-relevant log data from medical devices, looks for security vulnerabilities that can be inferred from the log data, detects patterns and events that qualify as potential security threats and creates security insights and proactive alerts to the respective stakeholders. The potential output of security analytics solution will consist of security alerts, aggregated statistics (security trends) and some insights that indicate the security posture of device environments and scope for improvement.

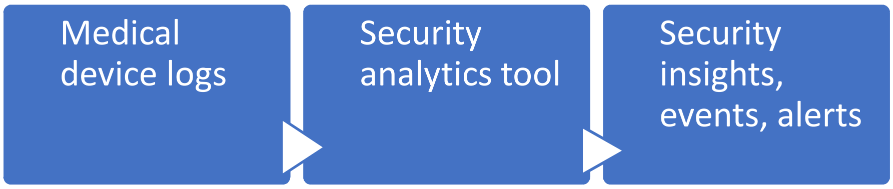


Figure 5 High level schematic view of e-health security analytics solution

In this section, data sources that provide input to the security analytics solution are first described and it is followed by the overview of the system design architecture of the solution. Finally, a global architecture is presented to show where the security analytics solution sits in the entire SAFECARE system.

5.1 Data sources

This section enumerates the different data sources considered in the e-Health device analytics solution. They include operating system logs, application logs, end-point security data sources (e.g. antivirus, firewall logs) and other external data sources (e.g. vulnerability databases). However, the state of art medical devices are typically not yet instrumented to act as a key source of security data. So, the current logging standards and mechanisms used in these devices do not capture all the security-relevant data from the devices. The proposed security analytics solution uses the log data that is currently available and gradually works towards proposing extensions to improve the logging mechanisms so that more security relevant data is logged by the devices. This will in turn improve the accuracy and comprehensiveness of security analytics solution.

The data sources that feeds input data to security analytics solution are as follows. We note that the analytics solution adheres to privacy by design and privacy by default approaches. Although most of the input data processed by the analytics solution is device data, (legacy) logs may contain some residual personally identifiable information (PII) of the device operators or the device manufacturer staff. De-identification of the input data takes place where PII data are removed before the data is fed as input to the analytics solution.

Operating system logs: Operating systems (OS) for medical devices, servers, workstations, and networking devices (e.g., routers, switches) usually log a variety of information related to security. The most common types of security-related OS data are as follows:

- System Events. System events are operational actions performed by OS components, such as shutting down the system or starting a service. The details logged for each event also vary widely; each event is usually timestamped, and other supporting information could include event, status, and error codes; service name; and user or system account associated with an event.

- Audit Records. Audit records contain security event information such as successful and failed authentication attempts, file accesses, security policy changes, account changes (e.g., account creation and deletion, account privilege assignment), and use of privileges. OSs typically permit system administrators to specify which types of events should be audited and whether successful and/or failed attempts to perform certain actions should be logged.

Application logs: Many applications generate their own logs. These may log to their own log files or log to OS logs. Examples include different log sources logging to the Windows event log and the Linux equivalents. Applications vary significantly in the types of information that they log. The following lists some of the most commonly logged types of information and the potential benefits of each:

- Client requests and server responses, which can be very helpful in reconstructing sequences of events and determining their apparent outcome.
- Account information such as successful and failed authentication attempts, account changes (e.g., account creation and deletion, account privilege assignment), use of privileges, and device configuration changes.
- Significant operational actions such as application startup and shutdown, application failures, authentications, access to sensitive files and functions, and major application configuration changes that require special privileges. This can be used to identify security compromises and operational failures.

End-point security sources: Medical devices may have pre-installed security applications for antivirus, intrusion detection (IDS), prevention and whitelisting. These applications are host-based while some others are network-based IDS. Such end-point security applications are useful in providing baseline security to medical devices. These applications record detailed information on suspicious behavior and detected attacks, as well as any actions intrusion prevention systems performed to stop malicious activity in progress. However, they are general purpose solutions which do not embed the intrinsic complexities and comprehensiveness of medical device infrastructures. Security analytics specialized for medical infrastructures in combination with such pre-installed security applications ensure robust security. Analytics over the security-specific data logged by security applications result in enhanced cyber security. The same applies to the correction functioning and status of these security applications themselves. Therefore, they are valuable data sources for the proposed security analytics solution. Some security applications generate their own log files, while others use the logging capabilities of the OS on which they are installed.

Other security information sources: There are also customer complaint and feedback databases that are used in addition to the above logs to find out more detailed information about security incidents and issues retrospectively for the purpose of forensic investigation, learning attack patterns or discovering recurring vulnerabilities.

Public vulnerability databases such as CVE MITRE database[9] are also useful resources to understand the existing vulnerabilities in medical devices and the patterns in which these vulnerabilities can be manifested into threats.

5.2 Security analytics architecture

The system architecture is described in Figure 6 below and in the rest of this section.

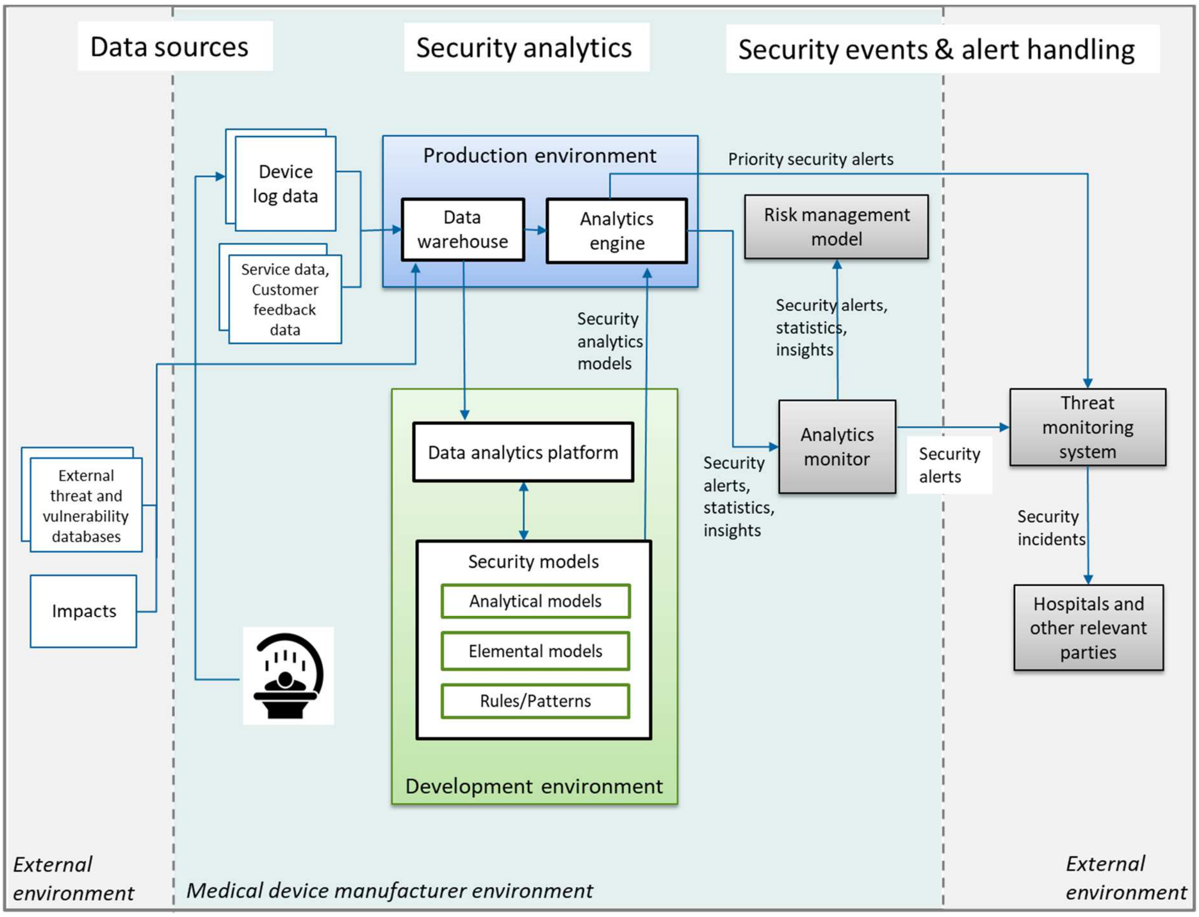


Figure 6 Security analytics architecture

The architecture of e-health device security analytics solution consists of three main functional segments:

1. **Data Sources**: This segment consists of all the data sources (both from internal and external environment) that provide input to the security analytics solution. The sources include
   a. device logs from medical equipment,
   b. service and customer[10] feedback data,
   c. data from external or public threat and vulnerability databases (e.g. Common Vulnerability Exposures (CVE) and common attack patterns prevalent in the context of medical devices),
   d. impacts from the SAFECARE impact propagation model.

[9] https://cve.mitre.org/

[10] The entity "customer" refers to the customer of a medical device manufacturer, e.g. a hospital.

2. **Security analytics**: The security analytics solution retrieves security-relevant data from the data sources, performs analytics over this data and outputs security insights and alerts upon detecting anomalous or suspicious security events. The internal working of the analytics solution is explained further in this section.
   Independent of this solution, medical devices may have a basic alert generator onboard to (also) alert the threat monitoring system when specific high critical events take place. Such a mechanism may bypass the device manufacturer's environment for immediate follow-up. This concerns events of high impact, low false positive probability and based on basic analytics models, e.g. based on log pattern matching or other rule-based approaches.
3. **Security event and alert handling**: The security events and alerts produced by the security analytics solution are handled by entities in two environments: medical device manufacturer environment and the external environment.
   The manufacturer environment consists of the analytics monitor that receives the output of the analytics engine which comprise of security event alerts, aggregated statistics and security insights. The analytics monitor reviews the output automatically or interactively with human. This step aims to reduce false positives and also to send the correct output to the intended parties. After the review, the analytics monitor performs three types of tasks:
   a. It forwards the alerts, statistics and insights to the medical device risk management model. The manufacturer uses the aggregated statistics and the security insights to improve the risk management model.
   b. It forwards particular alerts to the specific staff in the manufacturer environment. The staff may take corrective action (e.g. to correct configuration on specific devices) as part of remote product maintenance and service operation.
   c. It forwards alerts to the threat monitoring system in the external environment. The threat monitoring system checks if the alerts can be qualified as security incidents and provides a visualization of the incidents to the relevant stakeholders, for instance, hospitals.

   Priority alerts bypass the analytics monitor and are sent directly to the threat monitoring system in order to ensure minimum delay in making the security event or incident visible to the responders (e.g. hospital staff, SOC operators). This enables the responders to take immediate action and thus, minimize the extent of adverse consequences on the healthcare infrastructure.

5.2.1 Security analytics solution

The security analytics solution runs within the medical device manufacturer environment. This environment consists of production and development environments.

The production environment consists of two modules:

1. **Data warehouse**: The data warehouse is a high performance, highly scalable analytic database. Devices push logs over mutually authenticated secure channels to a data lake daily. The data is imported from these raw log files to the structured data warehouse. It includes a collection of threats, CVEs, common attack patterns and impacts that are

relevant to the medical device context. An SQL interface enables the retrieval of security-relevant data from the data warehouse that will be used for security analytics purpose.

2. **Analytics engine**: The analytics engine runs security analytics models on medical device log data coming from the data warehouse and generates an alert if security analytic models detect a security event. The models are developed by the data analytics platform in the development environment. The analytics engine runs the models at pre-defined times in a run-time environment. The detected events will further be checked by the analytics monitor which may include a review by human analysts. This ensures low false positive rates and high accuracy in threat detection by the security analytics models.

The development environment enables the development of security analytics models. The environment is arranged for interactive model development by security experts and data scientists. It consists of a data analytics platform and the security models developed by the platform. The description the platform and the resulting models is given below.

Data analytics platform: This platform runs a variety of data analytics solutions ranging from Python Scikit to R. It includes log filter which filters out from the huge volume of medical device log data the log entries that are relevant for assessing the security of medical device. Technically, the log filter queries the data warehouse for security-relevant data via the SQL interface that is available at the data warehouse. The analytics solutions residing on the platform analyze the output of the log filter and enable the development of security models. The simple models are based on static list of patterns stored within the platform or in the production environment's threat repository. Advanced analytical models are developed by applying machine learning and deep learning techniques.

Security models: The security models are developed by data analytics platform. The models include simple rules, patterns, elemental models and complex analytical models. The elemental models assess basic security features in the medical devices. The analytical models perform advanced analytics on the data and support complex attack patterns. The models are reviewed by security experts and data scientists who judge the accuracy. Then they decide either to push the model to the analytics engine in the production environment or to further iterate to improve the model.

5.2.2 Security analytics levels

There are two levels of analytics:

1. Analytics over a device population: At this level, security analytics is performed over a device population. A device population refers to a set of devices, for instance, a set of all the deployed medical devices in a particular geographical location and whose logs are available to the device manufacturer for the purpose of security analytics. Such analytics analyze the device population and provide statistical results such as how many devices are at a particular security risk at a particular period.
2. Analytics over individual devices: Here, analytics is performed on a specific device's logs to detect an actionable security situation, e.g. insecure configuration or suspicious event(s), occurring within that device. This level of analytics could be an extension of analytics done over a device population. That is, one could target a particular device within a risky device population and then perform in-depth analysis of the individual device logs.

5.3 System interconnections with SAFECARE components

This section describes the interconnections between the e-health device security analytics solution and other components of the SAFECARE system. It also presents the global architecture of the SAFECARE system to show where and how the security analytics solutions fits within SAFECARE.

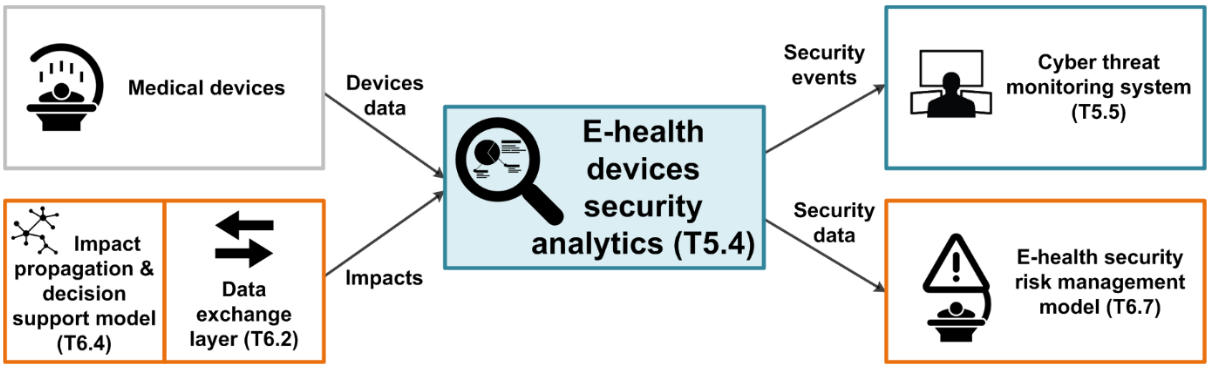
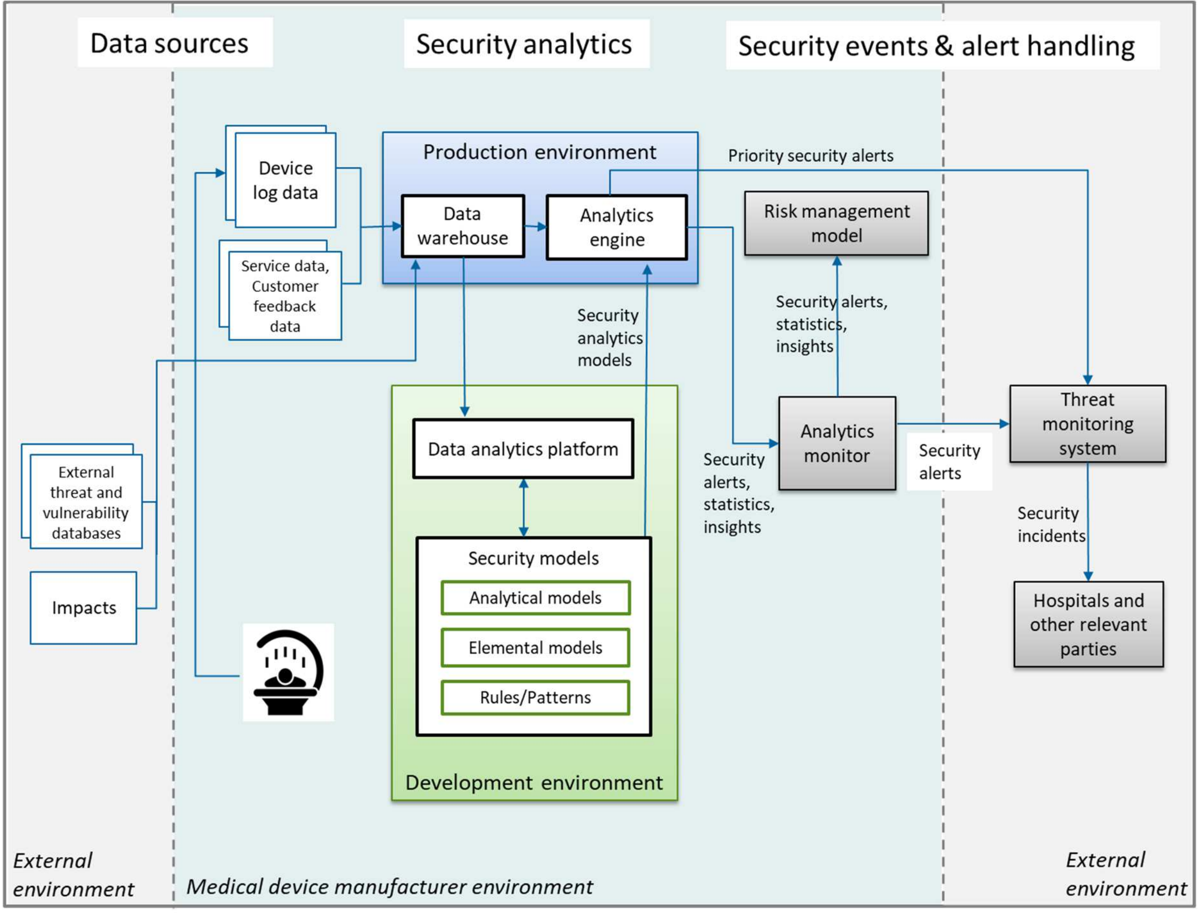

Medical devices
Devices data
Impact propagation & decision support model (T6.4)
Data exchange layer (T6.2)
Impacts
E-health devices security analytics (T5.4)
Security events
Cyber threat monitoring system (T5.5)
Security data
E-health security risk management model (T6.7)

Figure 7 Interconnections between security analytics and other components in SAFECARE

As shown in Figure 7, the security analytics solution (T5.4) has interconnections with

- **Medical devices**: The security analytics solution acquires log data generated by the medical devices and performs analytics over this data. The devices are manufactured by the device manufacturer and deployed at the hospitals. The manufacturers receive log data for maintenance, monitoring and product improvement purposes. This includes security purposes.
- **Impact propagation model (T6.4)**: The security analytics solution retrieves a list of impacts resulting from the impact propagation model via the data exchange layer (T6.2). These impacts could be used by the solution for post-incident analysis and to create new analytics models by leveraging the device manufacturer's development environment and its functions. The specification of the impact propagation model will be presented in the future deliverable D6.6.
- **E-health security risk management model (T6.7)**: Aggregated security insights, event alerts resulting from the security analytics solution are sent to the e-health device security risk management model. The purpose of the risk management model is to assess the security risk in medical devices. Analytics results are used for improving this risk management model and also to take appropriate actions based on the type of alerts. The specification of this risk management model will be presented in a future deliverable D6.12.

***Cyber threat monitoring system (T5.5)**: As depicted in Figure 6*



- Figure 6 Security analytics architecture, security alerts generated by the security analytics solution are sent to the cyber threat monitoring system. This system is responsible for centralizing the cyber security events from multiple security assets on a dashboard dedicated to SOC operators and other responder entities. This dashboard provides a global picture of cyber and physical security events and impacts to the SOC operators, assist them in better decision making and also improve investigation capacities by displaying relationships between "impacted" equipment and "monitoring" equipment. The specification of this threat monitoring system will be presented in the future deliverable D5.9.

5.3.1 Format of log data from medical devices

The types of log data and their formats are mentioned in the section Data sources. A brief summary of the formats is also provided here. In almost all cases, logs are in a proprietary format defined by the applications running on medical devices. In some cases, the logs may follow a common format, e.g. Windows event logs. In some other cases, it may follow a standard format, e.g. W3C extended log format for Windows host firewall logs.

5.3.2 Format of impact from impact propagation model

The security analytics solution interfaces with the SAFECARE component impact propagation model and uses the impacts resulting from this model as one of its inputs while creating new analytical models or to further analyze the impacts of detected security incidents. The format of such impacts is illustrated by the following example. This example has been provided in context of the development of the impact propagation model and will be documented in deliverable D6.6 “Specification of the impact propagation and DS models”.

```
{
  "Impacts":[
    {
      "IncidentID":"I1",
      "IncidentType":"fire_detection",
      "Assets":[
        {
          "AssetID":"ID1",
          "AssetName":"cardio_room",
                              "Risk_type":"fire",
          "ImpactScore":1
        },
        {
          "AssetID":"ID2",
          "AssetName":"computer room",
                              "Risk_type":"fire"
          "ImpactScore":0.8
        }
      ]
    },
    {
      "IncidentID":"I2",
      "IncidentType":"intrusion",
      "Assets":[
        {
          "AssetID":"ID2",
          "AssetName":"computer room",
                              "Risk_type":"intrusion"
          "ImpactScore":1
        },
        {
          "AssetID":"ID3",
          "AssetName":"computer",
                              "Risk_type":"unauthorized_access"
          "ImpactScore":1
        }
```

5.3.3 Format of a security alert generated by the security analytics solution

As mentioned in the section Communication interface requirements, the alerts generated by the security analytics solution are required to be in Syslog format and they will be sent to the SAFECARE cyber threat monitoring system using the Syslog protocol.

An example scenario is considered here to show the contents of an alert message and the format in which it will be shared with the threat monitoring system.

Scenario: The security analytics solution detects a malware infection on specific models of medical devices and generates an alert with the following title and attributes:

Alert: Malware detected on medical device model X

- Alert attributes:

- Detection sources: Antivirus and Security Analytics Solution
- Threat categories: Malware
- Severity: Medium
- Event detection timestamp: 20190410T165514Z
- Status: In progress

Consequently, the syslog alert message may look like this:

```
<Prioritynumber>20190410T165514Z Antivirus and Security Analytics Solution su PID messageID OtherStructuredData Malware detected on medical device model X
```

5.3.4 Format of a security incident sent by threat monitoring system to responders

An example for a security incident which is transformed from an alert by the SAFECARE threat monitoring system is provided here to illustrate the incident's format. The format will be specified in deliverable D5.9 "Specification of the cyber threat monitoring system".

```
Incident
{
   "description": "Malware",
   "detector": "Antivirus and Security Analytics Solution",
   "last_modification_date": "20190410T165514Z",
   "last_reception_date": "20190410T165514Z",
   "severity": "MEDIUM",
   "start_date": "20190410T165514Z",
   "title": "Malware detected on medical device model X",
   "type": "INCIDENT",
   "unique_identifier": "A#85647",
   "assets": [
      {
         "category": "TARGET",
         "name": "medical device model X"
      }
   ],
   "total": 1
}
```

5.4 Security analytics in SAFECARE global architecture

The E-health device security analytics solution is one of the cyber-security solutions in SAFECARE. Figure 5 shows where the solution sits in the global architecture of the SAFECARE system. It depicts all the physical security solutions, cyber security solutions and integrated solutions within SAFECARE and the interconnections between them. The future deliverable D6.1 will provide the specification of the global architecture. For more information about the global architecture, D6.1 should be referred.

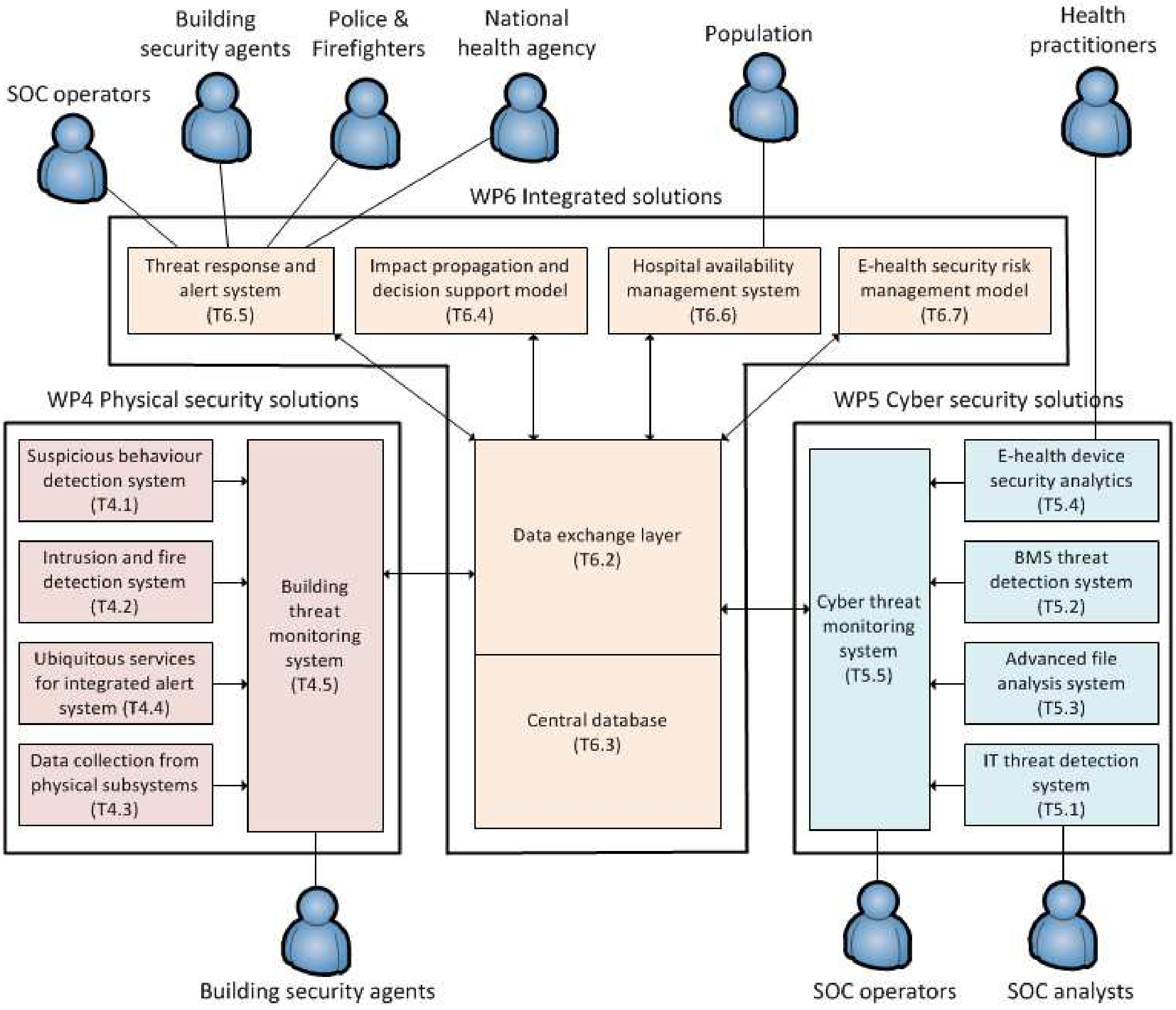

Building security agents
Police & Firefighters
National health agency
Population
Health practitioners
SOC operators
WP6 Integrated solutions
Threat response and alert system (T6.5)
Impact propagation and decision support model (T6.4)
Hospital availability management system (T6.6)
E-health security risk management model (T6.7)
WP4 Physical security solutions
Suspicious behaviour detection system (T4.1)
Intrusion and fire detection system (T4.2)
Ubiquitous services for integrated alert system (T4.4)
Data collection from physical subsystems (T4.3)
Building threat monitoring system (T4.5)
Data exchange layer (T6.2)
Central database (T6.3)
WP5 Cyber security solutions
Cyber threat monitoring system (T5.5)
E-health device security analytics (T5.4)
BMS threat detection system (T5.2)
Advanced file analysis system (T5.3)
IT threat detection system (T5.1)
Building security agents
SOC operators
SOC analysts

Figure 8 Global architecture of SAFECARE system with E-health device security analytics

6 Security analytics models

The objective of security analytics solution is to perform analytics on the data from the medical devices and develop analytics models that detect various medical device security events and generate alerts. Some example medical device security events that could be detected and reported by the security analytics solution are given in **Erreur ! Source du renvoi introuvable.**. This list is based on NIST SP800-81 Revision 2[11] and adapted from a white paper[12] on cybersecurity in medical devices.

Event	**Description**
Malware on device/systems	Malicious software (e.g. Virus, Worm, Trojan, and Ransomware) introduced into medical devices or other systems in the hospital network.
Device, application, configuration or software manipulation	Device, software or configuration settings modified producing unpredictable results. This can result in hardware and software failures in the medical equipment.
Denial of control action	Device operation disrupted by delaying or blocking the flow of information, denying the availability of either the device or networks used to control the device to the hospital staff.
Device functionality manipulation	Unauthorized changes made to embedded software, programmable instructions in medical devices, alarm thresholds, or unauthorized commands issued to devices, which could potentially result in premature shutdown of devices and functions or even physical damage to equipment (if tolerances are exceeded).
Safety functionality modified	Safety-related functionality manipulated such that they do not operate when needed; or perform incorrect control actions, potentially leading to damage to medical equipment or physical harm to patients or hospital staff.
Spoofed device/system status information	False information sent to operators either to disguise unauthorized changes or to initiate inappropriate actions by the hospital staff

[11] **NIST. 2015.** *Guide to Industrial Control Systems (ICS) Security.* 2015. Special Publication 800-82.

[12] **Richard Piggin. 2017.** *Cybersecurity of medical devices: Addressing patient safety and the security of patient health information.* s.l. : BSI group, 2017. White paper.

Table 2 Medical device security events

To demonstrate the feasibility of device security analytics approach, some early experiments have been conducted which have resulted in the following proof of concept analytical models:

- Status of security functions: This model checks the current status of security the anti-virus definition files[13] running on medical devices. Particularly, it detects devices for which the virus definition files do not update and get outdated. Thereby, the model provides an overview of devices that pose a security risk due to the sub-optimal functioning of this security function. The experiment shows that analyzing the security-related logs from the devices can enable this model with a high degree of accuracy and ability to take corrective action.
- Security of environment: This model assesses the security environment of medical devices based direct exposure of devices to outside the protected hospital network and frequency of virus detections on USB media. The experiment shows that medical devices can act as a security sensor in hospital environments and can provide actionable results.
- Security feature usage: an experiment was successfully performed to determine the actual authentication workflow of a medical device. This demonstrated that a very small minority configures the optional more secure authentication. It further demonstrates that even this minority does not use the feature as intended. This kind of information is valuable input to the security risk management model and may be used in product and security feature development towards effective security.

The proof-of-concepts above are to be further developed and implemented as part of deliverable D5.8 "E-health devices security analytics".

[13] The data sources for the security analytics solution include end point security sources such as anti-virus software which consists of virus definition files.

7 Conclusion

This deliverable provides the specification for the E-health devices security analytics solution. It describes the architecture of the solution to be realized and demonstrated in SAFECARE context. The architecture covers the security analytics solution, the end-to-end infrastructure and security analytics models. It furthermore covers how these integrate with and feed into SAFECARE threat and incident management workflows, product support workflows and security risk management models and processes.

The specification takes into account the requirements and scenarios presented in this document, which build on SAFECARE deliverables D3.4 "Initial requirements analysis" and D3.6 "Definition of the cyber-physical scenarios of threat" respectively.

Early experiments with an incomplete infrastructure and available medical device log data demonstrate that E-health device security analytics is a practical and effective approach.

The next step will be the realization of the specification and delivering the E-health devices security analytics prototype (Deliverable D5.8).