SAFECARE

Integrated cyber-physical security for health services

Specification of the Threat Response and Alert System

Deliverable 6.8

Lead Author: ENOVACOM

Contributors: CSI, CNAM, AP-HM, ASLTO5, AMC, SPF, KEMEA, FMI, SGSP

Deliverable classification: (PU)

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

Version Control Sheet

Title	Specification of Threat Response Alert System
Prepared By	*ENOVACOM*
Approved By	
Version Number	*1.5*
Contact	David Fermet, Frédéric Nodot, Cyril Garde

Revision History:

Version	Date	Summary of Changes	Initials	Changes Marked
0.1	21/10/2019	Draft Version	ENC	
1.0	28/11/2019	Initial Version	ENC	
1.1	6/12/2019	Apply proper font to template style	ENC	
1.2	13/12/2019	Adding FMI contribution	FMI	
1.3	13/12/2019	Corrections after ISEP's review	ENC	
1.4	17/12/2019	Integration of KEMEA's contribution	KEMEA	
1.5	19/12/2019	Corrections after AMC's review	ENC	
1.6	19/12/2019	Corrections after CSI comments	ENC	

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**
DXL	Data Exchange Layer
MAS	Mobile Alerting System
CDB	Central Database
BTMS	Building Threat Monitoring System
CTMS	Cyber Threat Monitoring System
SMS	Short Message Service
TRAS	Threat Response and Alert System
PBX	Private Branch Exchange – Phone system
SBC	Session Border Controller
MQTT	Message Queuing Telemetry Transport
API	Application Programming Interface
EAI	Enterprise Application Integration

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 project 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 tools 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.

Executive Summary

This deliverable covers the specification of the Threat Response Alert System (TRAS), as part of Work Package 6 "Integrated cyber-physical security solutions".

As referred to in the DOA, a curated list of objectives to meet and their related KPIs, narrowed down to TRAS contribution, is the following:

Table 1 – TRAS DOA's respective objectives & KPIs

Ref	Objective	KPI
07	To improve **threat response capacities:** defense strategies, reaction cards, automated processes (bpm).	● KPI7.1: Time to respond without and with the project solutions ● KPI7.2: Number of involved security practitioners to carry out the incidents without and with the project solutions
08	To improve **impact mitigation capacities:** manage hospital availability, inform the population, and increase user awareness about impacts on critical assets.	● KPI8.1: Time to mitigate the impacts and come back to a normal state without and with project solutions ● KPI8.3: Time to notify the relevant user communities (security teams, public authorities)

Threat Response and Alert System is an automated communication platform whose role will be to implement the communication tasks of reaction plans. The objective to reach is to provide end users with an adaptative yet efficient notification and alert system so that they can act swiftly upon each risk assessment. Impact Propagation Model is a key component of the solution as it provides a computed vision on potential risks, based on upstream alerts from the cyber & building detection systems. These risks are expressed in terms of potentially impacted assets, risk type & severity as well as a risk score. They will then be associated automatically – against business rules – to the corresponding reaction plan designed by the hospitals, thus bridging the gap between all the automated detection / impact computation and the stakeholders in charge of prevention or event mitigation. Therefore, it is expected that stakeholders will be informed in a very short time after a risk is detected, and reaction plan details will be executed so as to reach the swiftness expectation.

The deliverable provides a functional description of TRAS, its dependencies with other SAFECARE modules, and some detailed examples of reaction plan implementation possibilities. A focus will be made on implementation, especially on the project management methodology, so as to organize the implementation phase in such a way that we can measure the efficiency of the overall solution. It details the preparatory work required by the hospital, as to specify in detail reaction plans for each threat scenario.

Interconnections with other SAFECARE modules will be detailed, mainly by cross-referencing relevant specifications, so as to gather technical implementation details.

1 Introduction

This section presents an overview of the functional aspects, an interaction overview with other SAFECARE components and a high-level architecture.

1.1 Functional overview

As of the Description of Work, the Threat Response and Alert System (TRAS) is a rule processing engine designed to be able to parse the output of the Impact Propagation Model module and execute all communication related to the reaction plan to execute in answer to the given impact.

TRAS will execute all notification and alerts tasks, including the ability to send SMS, email, place interactive voice calls and process SMS answers. An interface is expected with the Mobile Alert System to be able to push notifications to mobile users as well.

TRAS objective is to improve coordination between internal and external security practitioners. It aims at improving recovery time or preventing an event from occurring through fast and efficient alert delivery.

An important part of the implementation phase will consist in determining with the end users the notification and alert strategies to put in place, as the system will only be able to execute predesigned alert and notification patterns. This work requires the adaptation or the writing of procedures and should be an extension of an existing Activity Continuity Plan already in place in each Hospital. The difference being that existing plans may not have encompassed all the scenarios of the SAFECARE project.

The solution will be designed to be able to carry out “small” alerts (e.g. including a few people to notify, alert) as well as large alerting plan. The expected sizing should be able to address thousands of people within minutes and provide an efficient mobilization plan within the hour.

1.2 Interaction overview

As stated in D6.1 “Specification of the global architecture”, the interconnections of the Threat Response and Alert System with the other SAFECARE components is detailed in the following figure:

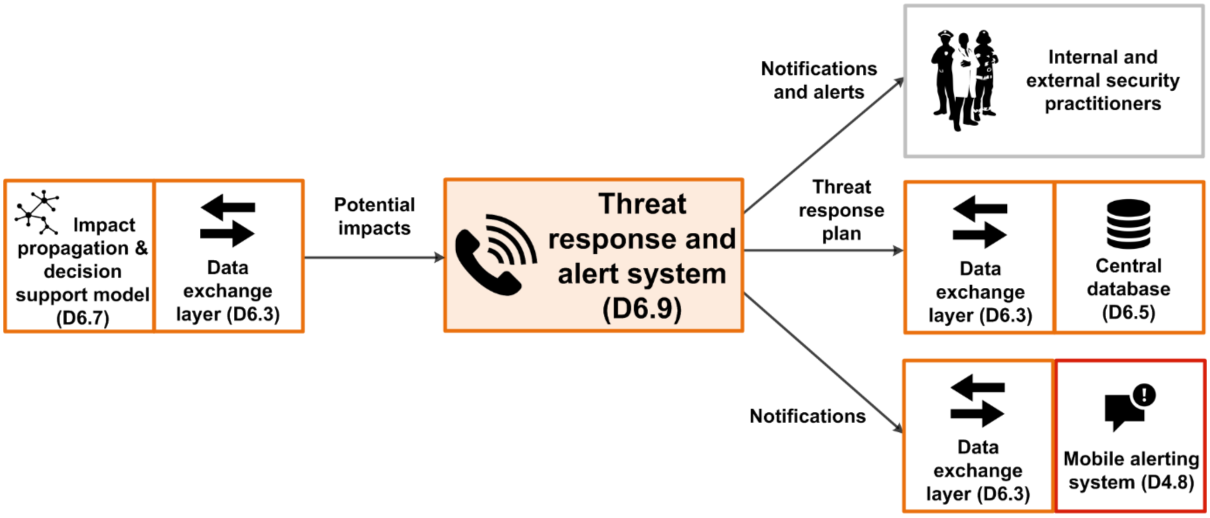
Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Potential impacts
Threat response and alert system (D6.9)
Notifications and alerts
Internal and external security practitioners
Threat response plan
Data exchange layer (D6.3)
Central database (D6.5)
Notifications
Data exchange layer (D6.3)
Mobile alerting system (D4.8)

Figure 1 – Interconnections of the threat response and alert system

The following table provides complementary details on each interaction:

Table 2 – Interaction details

Interaction	Details
Potential impacts	Received from Impact Propagation Mobile (IPM) over the Data Exchange Layer (DXL). Impact messages will detail the list of assets, each being associated with a given risk and probability score. These messages will be associated to a Reaction Plan, as defined by the implementation hospital, mainly based on the assets, risks and probability score.
Notifications and alerts	TRAS will execute the communication tasks, using third party providers to carry out communication to the relevant users.
Notifications	Notification messages will be sent to the Mobile Alerting System (MAS), to warn their users of a given response plan execution and calling them for action. As for TRAS, MAS is another media that will be included in the Data Mining phase with each hospital. As detailed in 'D4.7 Mobile Alerting System specification', the mobile application will allow several user interactions: • Notification with no user feedback • Notification with simple acknowledge (or dismiss) • Notification with accept / reject feedback Notification sending from TRAS to MAS will go through DXL.
Threat Response Plan	The result of a response plan execution will be sent back for storage in the Central Data Base via the Data Exchange Layer.

1.3 General Architecture overview

The Threat Response and Alert System is a multitenant cloud-based platform, designed for high performance communications.

The following figure details the main modules of TRAS and its integration with SAFECARE components.

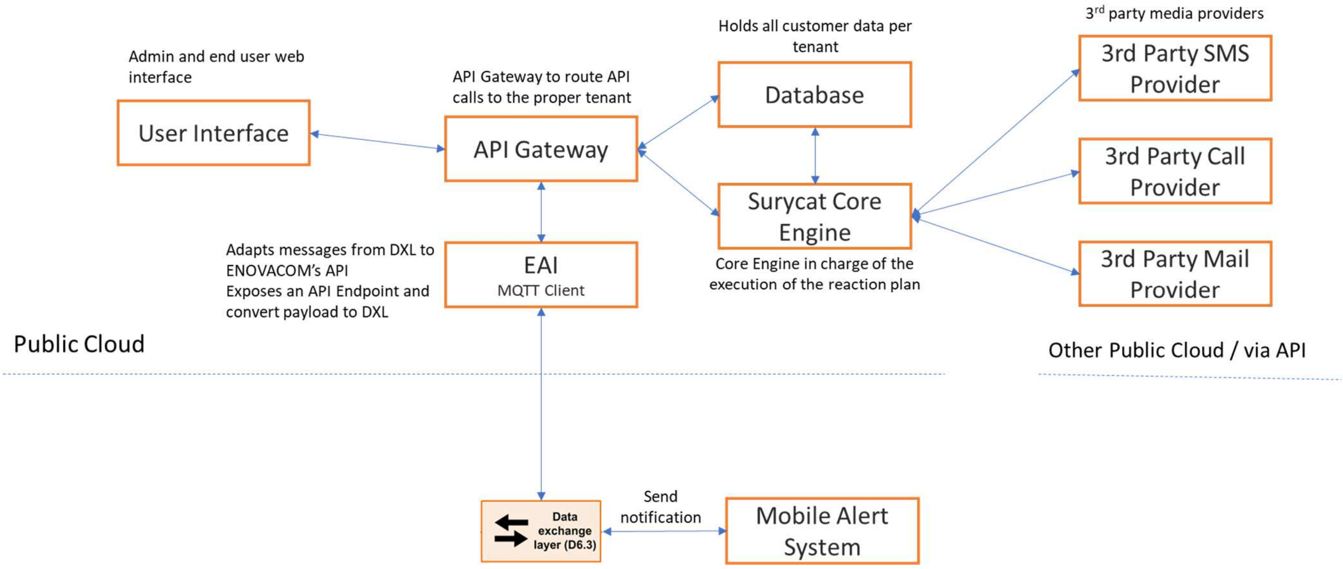
Admin and end user web interface
User Interface
API Gateway to route API calls to the proper tenant
API Gateway
Holds all customer data per tenant
Database
Surycat Core Engine
Core Engine in charge of the execution of the reaction plan
3rd party media providers
3rd Party SMS Provider
3rd Party Call Provider
3rd Party Mail Provider
Adapts messages from DXL to ENOVACOM's API
Exposes an API Endpoint and convert payload to DXL
EAI
MQTT Client
Public Cloud
Other Public Cloud / via API
Data exchange layer (D6.3)
Send notification
Mobile Alert System

Figure 2 – Threat Response and Alert System global architecture

The solution is cloud-based, GDPR compliant, multi-tenant and scalable.

It relies on a serverless & managed container combo, all of which addressable via an API.

A user interface is available for users to manage their environment: address book, workflow configuration, access to reports, …

A Database will store all tenant relative configuration information such as contact data (from address book), workflow configuration and settings and report data). Data is isolated per tenant.

The Core Engine is in charge of workflow execution upon the reception of a triggering message.

The EAI module is in charge of interfacing with the Data Exchange Layer:

- converting MQTT messages into API calls after a few treatments (such as replacing static data IDs by values, …).
- Polling static data to provide quick reference translations
- Returning Threat Response Plan to the central database once alerts & notifications are fully processed
- Sending notification requests to Mobile Alert System

2 Functional specification

Functional specifications will cover all the main features of the TRAS. From the type of data that is expected from the Data Exchange Layer, concepts used to store reaction plan stakeholders contact information (address book) to all the functional components required allow a customizable implementation of a reaction plan.

2.1 Input Data as events

According to documents ‘D6.1 - Specification of the global architecture’ and ‘D6.2 - Specification about Data Exchange Layer', the TRAS module will be a consumer of Potential Impact messages that are generated by the IPM module and made available by the DXL component.

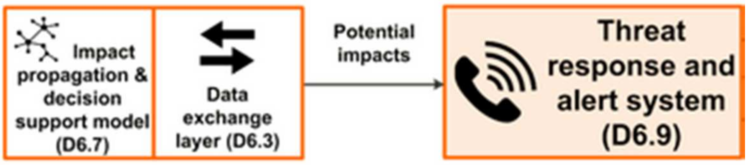
Impact propagation & decision support model (D6.7)
Data exchange layer (D6.3)
Potential impacts
Threat response and alert system (D6.9)

Figure 3 – Input Interconnection of the threat response and alert system

These messages report which assets are threatened by a single incident and with which degree of severity.

An asset is a physical element of the hospital that could be attacked. It can be for instance a medical device, a door, a computer etc. It is identified in the SAFECARE SYSTEM by a unique SAFECARE ID.

The Impact message must provide for each asset at risk the following data:

1. The threatened asset;
2. The threat on the asset;
3. The risk score of threat occurrence.

The risk score should be represented as a value going from 0 to 1, where 0 means negligible risk and 1 means maximum risk. This score reflects both the likelihood and the severity of the incident on the asset.

In order to get all the relevant information to process the Impact Propagation message, a table will be stored in the TRAS module. This table will link all the real-world information of the asset such as name, category, location etc. with its SAFECARE ID.

The static data from this table will be retrieved regularly from the CDB module.

2.2 Address book

The TRAS relies on an address book to send alerts and notifications. The solution will hold a separate, self-hosted, copy of the hospital’s address book so that in case of an incident impacting the hospital’s IT, recipient information is still available.

The project management phase will determine the list of contact to import on the platform.

Each contact will have a few information:

- Medias: list of all relevant phone numbers, mobile phone numbers, email addresses, and if relevant home and business address (for location-based group selection)
- Tags: adds the possibility to import existing qualifiers or add custom ones to help select a group of contact based on tags (such as profession, membership to a given response group, …)

TRAS address book can be manually imported, but it is highly recommended to proceed to an automated synchronization with the existing software of Human Resources. The project phase described in chapter 3.3 presents a recommended methodology.

2.3 Global workflow specifications

A workflow is a logical description of a reaction plan. The system will be designed in such a way to be able to represent and execute the communication logic for notifications, alerting and personal mobilization.

A workflow is composed of several "tasks", each task being a functional block in charge of either providing a business logic function or a communication function. Tasks will be linked together so as to represent a reaction plan logic (as a sequence flow), and the solution will provide a web user interface to create, modify and delete workflows. Table *3* – Concept definitions lists the main alerting functional blocks that are usually employed in reaction plans.

The workflow editor to be provided intends to make it possible for a user to implement its reaction plans, starting from the concepts up to the detailed implementation, task by task.

Table 3 – Concept definitions

Concept	Definition
Notification	Simple message sending with no user feedback
Alerting	Important message sending with explicit user acknowledge answer required
Mobilization	Alerting variant, asking for people to either accept or reject an instruction message (i.e. come back to hospital: available / not available)
Escalation	Either a notification / alerting / mobilization following an alerting or mobilization phase whose answer level does not meet the minimum quorum expected. Escalation is usually performed on a different group than the previous phase

2.4 Business Logic Tasks

Business logic tasks are technical tasks whose purpose is to manipulate or evaluate data.

It can be either evaluating input data such as the impact event, or the number of people who accepted and alert, to determine what task comes next, the message to be sent of the number of persons left to call.

All the business logic tasks are detailed in the following table:

Table 4 – Business Logic tasks

Task type	Description
Factory	For data manipulation. Sub tasks available: • Variable creation • Data field deletion

	• Data field copy • Data extraction using regular expressions • Data replacement (using lookup table) • Arithmetical operation • List merging • Conditional block (using the above tasks)
Recipient selection	Determines a list of persons to be concerned with upcoming communication tasks
Juncture	Set to wait all of a given subset of parent tasks. Can be used to synchronize communication phases
Wait	Basic waiting task, pausing upcoming actions for a given time
Task selection	Provides a conditional task selection, allowing conditional implementations
Trigger a workflow	Allows workflow inclusion, useful when coping with complex or repetitive patterns

2.5 Communication tasks

Communication tasks intend to send a message to a given user and eventually collect his feedback.

Communication means to be implemented are: SMS, phone call and email, as stated in the DoA. These are conventional communication means, easily adaptable to each hospital.

2.5.1 Communication: SMS

SMS tasks provide the ability to send a text message by SMS to a given recipient list.

Recipients can be set in the task in a static fashion or by an upstream business logic task that for instance provided some conditional logic.

The solution is designed to be able to send tens of thousands of SMS within minutes, by the integration of a third-party SMS provider. These providers offer several operation connection entry points in every country, therefore ensuring a very high level of availability.

The message to be sent will be based on a template – to be defined with end users - i.e. a combination of static text and dynamic elements, such as contextual information from the originating Impact message from IPM.

Message templates will be designed with the end users, as an important part of the project management phase, as they will carry all the required information the stakeholders will receive to mitigate / prevent impacts. Recipients should mainly be instructed to a course of action rather than simply be informed.

SMS are fast, but not highly reliable. Industry standards delivery rates are around 95% within a day. It has been observed that between 80 to 90% of SMS to be sent are received in the 5 following minutes in a normal situation (mobile network-wise). It can be used for all communication purposes but needs to be backed up in case of alerting or mobilization to compensate the potential bias in delivery.

SMS can be answered by their recipient. Their answer will be parsed and given syntax condition can result as a positive, negative or unknown feedback.

2.5.2 Communication: email

Emails should not be considered for alerting and mobilization, but rather of a way to have complementary and more detailed information in parallel of an SMS / voice call alerting workflow.

Email redaction is based on the same template concept as SMS.

Solution is designed to be able to send hundreds of thousands of emails within minutes. Integration with the hospital mail server is not required (so that mail delivery can be performed even if the mail server is down, as a direct or collateral target of an attack), but the hospital domain name can be used if need be, to improve trust on message reception.

Answering an email has not been implemented as it is not reliable in terms of delivery time.

2.5.3 Communication: Voice Call

Voice call are particularly efficient for alerting and mobilization. More reliable than SMS and emails to get people's attention, they are however slower to process.

Voice call can be described in quite every fashion to be interactive with the user. Table *5* – Voice call specific tasks lists all the building blocks to be used to design a phone call:

Table 5 – Voice call specific tasks

Task type	Description
Dial	Dial a phone number with a given dial timeout
Say	Uses text to speech synthesis (many languages available) to say a voice message from a text input. Text message to be said must be adapted and should avoid acronyms.
Play a sound file	Play a pre-recorded sound file
DTMF	Ask for the user input, using the user's phone keys. Can be used to enter a code, make a choice or confirm / reject a prompt
Hang up	Hang up the call and conditionally set the call status

A voice call can be described like a workflow, with all the business logic tasks, by using variables and conditional branches.

2.5.4 Communication: Mobile Alert System (MAS)

Communication tasks will be extended to Mobile Alert System, as detailed in 'D4.7 Mobile Alerting System specification'.

Mobile Alert System is to provide a complementary notification and alerting channel to given users.

As detailed in the specification document, Threat Response notification will be sent to mobile users.

The following table describes the potential notification delivery method and the related functional behavior:

Table 6 – Mobile Alerting System notification delivery and user interaction

Delivery method	Expected behavior
Notification *Simple message delivery with no expected user feedback*	MAS will receive the notification message from DXL whose delivery method will be "notification". The message will be pushed to the specified users, allowing them to read the message without any further interaction. MAS will send a notification response to DXL indicating that the message has been delivered.
Acknowledge *Message delivery with explicit user acknowledge expected. Falls back to "no answer" state after timeout*	MAS will receive the notification message from DXL whose delivery method will be "acknowledge". The message will be pushed to the specified users, allowing them to read the message once they acknowledge its reception. Users then commit to do something about the message received in a configurable timeframe. If the user has not acknowledged the message in the given timeframe, MAS will send back a response indicating that the message has been delivered but not acknowledged.
Confirmation *Critical message delivery with user accept/reject status expected. Falls back to "no answer" state after timeout*	MAS will receive the notification message from DXL whose delivery method will be "confirmation". The message will be pushed to the specified users, allowing them to read the message. While viewing the message, they can either accept or reject it, indicating they respectively commit to do something about the message received or that they are unavailable to do so. If the user has not answered the message in the given timeframe, MAS will send back a response indicating that the message has been delivered but not acknowledged.
- *Error handling*	Any other situation impairing MAS to delivery the message to the users, MAS will send back a notification response indicating the delivery status as failed, and provide an error description

2.6 Threat Response examples

The following sections provide a detailed implementation example of functional blocks as listed in Table *3* – Concept definitions.

2.6.1 Example 1: notification

Notification tasks is set to send an email & SMS to a given recipient list.

Logic flow is as follows:

- Configuration tasks: sets some static data such as sender name
- Group selection « tout le personnel » (all staff): selects every person in the address book

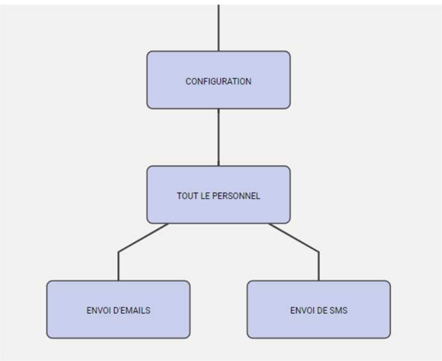

Figure 4 – Notification example

2.6.2 Example 2: Alerting

This workflow is designed for alerting, with the following characteristics:

- Conditional group selection: based on tag criteria for instance
- "Message": sets the message to be sent across various medias
- « Info début campagne » is a notification message sent by SMS to the crisis cell recipient group, to inform them the alerting campaign has been started
- "Envoi d'email" (email sending), "Envoi de SMS » (SMS sending) send SMS and emails to the target recipient group
- "Campagne d'appel" completes the SMS/email sending by a voice call, playing the same message but asking callees to acknowledge message reception (to distinguish voice mail from humans)

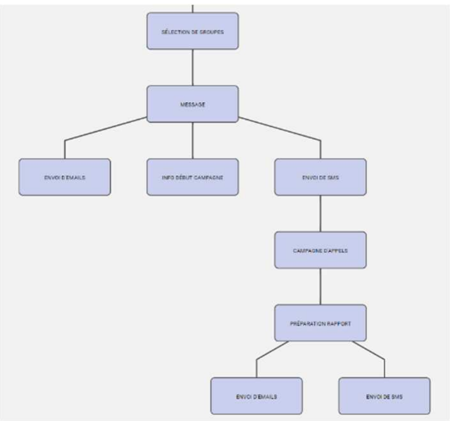

Figure 5 – Alerting example

"Preparation rapport" and the downstream tasks intend at preparing a simple report to be sent to the crisis cell group, letting them know how many contacts have been reached and the percentage of which acknowledged the message

This workflow example could fit a simple – low level – alert scenario, where the crisis cell group – or whichever group in charge of the event follow-up – can be informed in real-time that the alert has been sent off and get a synthetic report, providing them with the information needed to decide the next actions to undertake.

2.6.3 Example 3: Crisis Cell mobilization

The following workflow is intended for people mobilization, i.e. informing a recipient group of a given situation, and asking them to gather in team to organize the incident response.

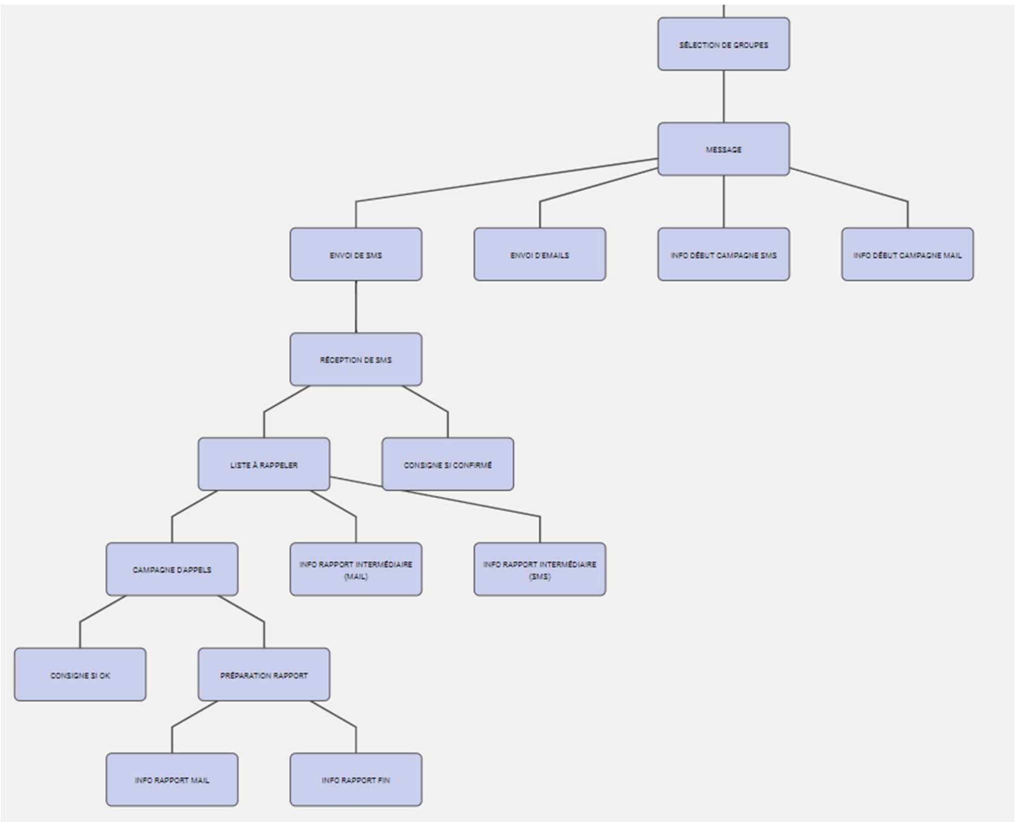

Figure 6 – Mobilization example

Tasks will not be described in detail, but the overall logic is as follows:

- Recipient group is set to crisis cell.
- Another group (here, the hospital board for instance) will be informed that the crisis cell is being mobilized
- Recipient group will first receive a SMS, informing them – in short – that the crisis cell is being mobilized and that that their presence is required. They will be able to answer this message indicating their availability
- If no answer is received in a given timeframe, the users will then be called, and asked the same question by phone.
- Eventually, a simple report will be built and sent to the "hospital board" group, giving them overall details on the mobilization results, especially how many persons confirmed their availability

2.6.4 Example 4: Combinations

The following example illustrates a combination of several alerting & mobilization workflow, each branch concerning a given service in the hospital.

The example is based on a conditional expression to determine whether or not triggering the alerting of an organizational group.

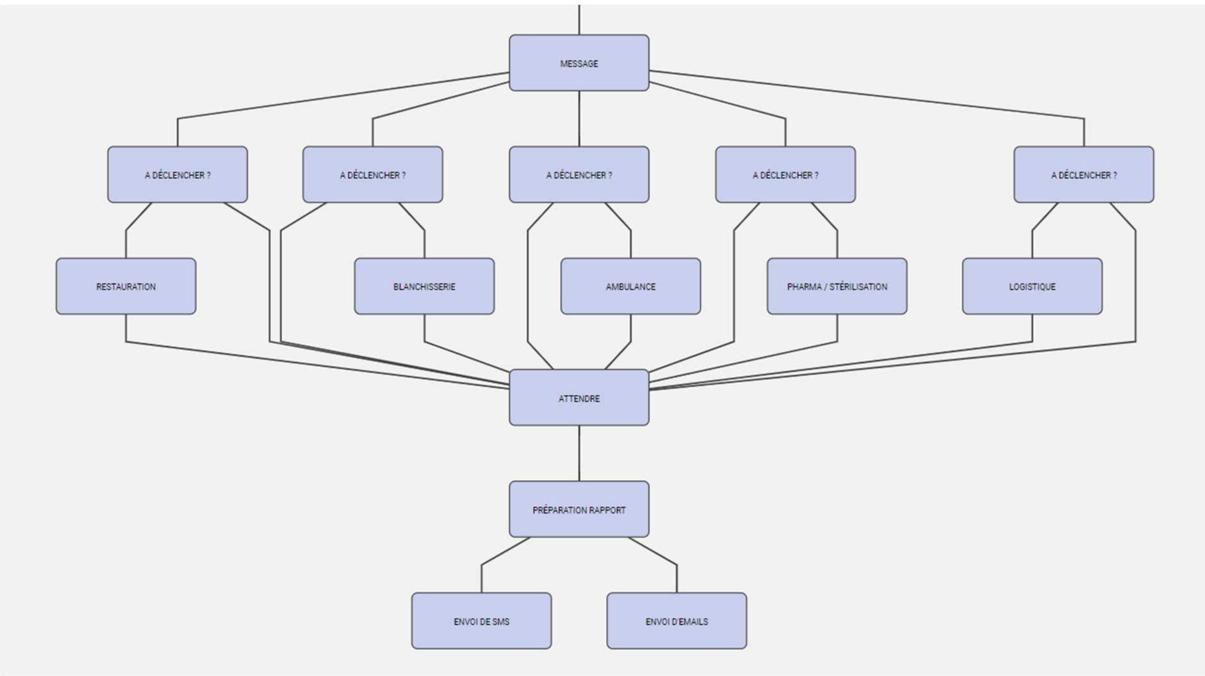

Figure 7 – Combination example

This example perfectly illustrates the association of business logic and workflow combination. For instance, the "Ambulance" sub-mobilization workflow will only be triggered if a given condition is met. Namely, if the triggering event payload meets the condition (like a score threshold and a given keyword presence)

2.6.5 End user customization

These examples are merely provided as potential guidelines. Section 3.3 will detail the methodology to be used to make the link between IPM output and the required organizational response expected by the stakeholders.

The stakes are to be able to provide a reliable and simple way to map a response procedure to a (potentially) highly polymorphic impact message.

3 TRAS implementation

The following sub-sections will detail what steps need to be conducted to implement TRAS in a hospital environments, starting by stating general concepts, choosing between a few architecture options and going through the project methodology to "translate" reaction plans – as on-paper procedures – into an actionable workflow logic.

3.1 Main overview

TRAS implementation will consist in two phases:

1. Technical implementation: setting up the tenant for the hospital and proceeding to all requirements implementation.
2. Functional implementation: starting from the demonstration scenarios, the hospital will constitute a work group in charge of defining all corresponding reaction plans. A few workshops will be organized with this work group to determine all functional aspects of TRAS configuration, namely:
    a. Identifying all stakeholders and getting their respective contact information;
    b. Determining the most suitable communication method (see §2.6) in each and every possible situation (based on the impact messages);
    c. Writing all message templates.

3.2 Architecture options & requirements

TRAS base architecture is purely cloud, with one potential integration option regarding voice call handling.

SMS, emails and calls use third-party providers, and all communications originate from outside the hospital. It is however possible, given some requirements, to integrate with the hospital PBX to make direct calls to phones that cannot be reach from the public phone network.

3.2.1 Full Cloud

In a full cloud deployment option, the following integration requirements will apply:

- Each contact phone number must have the E164 format, i.e. be reachable from the public phone network and respect the international format.
- Connection to Data Exchange Layer is possible from a cloud-based client, i.e. all ports and security settings are properly set to allow an external connection.
- To use the hospital domain as email domain by TRAS, some configuration on the domain provider is required so as to allow domain delegation with the third-party email service used.
- IT proxy / firewall settings will be tuned to allow the required user accessing TRAS user interface.

All technical integration aspects will be tested during the test phase and implementation at hospitals.

3.2.2 Hybrid

A hybrid cloud deployment option consists in making it possible to send internal call (i.e. to phone number not reachable by the public network, but only through the hospital PBX, using internal directory addresses).

Requirements in such a configuration are the same as for the full cloud option, plus:

- A SBC is available and configured to accept call origination from the TRAS third-party call provider;
- Configuration and licenses are setup in both SBC and the PBX network to allow call routing from TRAS to the required recipients.

This configuration option is not mandatory and will essentially depend on the need to call unreachable phones and the readiness of the hospital phone network to meet these requirements. Relying on internal phones to carry the alert message will have to be backed up in case the hospital PBX is down.

3.3 Project Management

The following sections detail the project methodology to follow for each implementation.

3.3.1 Data mining: end user threat response procedures

Data mining is the cornerstone of TRAS efficiency. The main implementation stakes will be to determine in a deterministic way a list of reaction plans, procedures, for all possible risks and impacts, for each considered scenario.

This work can only be done by the hospital. A work group will be set up to write these procedures down based on their study scenario and related assets.

3.3.2 Progressive & comprehensive workshops

So as to reach the functional objective, a few workshops will be conducted with each hospital.

The proposed methodology will consist in 3 workshops:

- Workshop 1: Specification
- Workshop 2: Dry-run
- Workshop 3: Drill

Table *7* – Implementation workshops provides detail for each workshop.

Table 7 – Implementation workshops

Workshop	Requirements	Objectives
#1	Hospital has constituted a workgroup and has written all reaction plan for each scenario, determining to course of action to undertake for each stakeholder. These documents will be communicated to ENOVACOM. ENOVACOM will demo the solution based on example scenarios so that the work group is made aware about the workshop's objectives	The first workshop objective is to layout all reaction plan details in terms of: • Listing all stakeholders and their contact information at best. A minimal objective is to determine all required stakeholders and figure out a way to provide their contact data for workshop 3; • Verifying the consistency of the reaction plans in regards of the potential impacts of the scenarios; • Choosing all communication options and write all message templates.

#2	Uses text to speech synthesis (many languages available) to say a voice message from a text input. Text message to be said must be adapted and should avoid acronyms.	The second workshop objective is to test and adapt - if need be - the specification. Each response plan will be triggered using simulated inputs, and the workgroup will play the role of the target stakeholder. It is expected to review all relevant impacts for each scenario to make sure of the overall functional implementation consistency. During this workshop, all aspects regarding the last workshop preparation will be reviewed.
#3	All parties involved in the drill will have been properly informed of the project details: reaction plans will have been shared and commented amongst them and they will have been informed of the drill details. All stakeholders contact information will have been gathered and sent to ENOVACOM for implementation. Legal, social and organization related aspects will have been covered by the hospital.	The third workshop's objective is to validate TRAS implementation in a real simulation, involving all parties. Final adjustments will be made following the drill, based on the feedback of experience to be conducted by the hospital work group. All TRAS users will be trained on the user interface during the exercise

4 Reaction plans

This section provides some insights in terms of reaction plans to be implemented, as well as Greece and France expectations on the matter.

TRAS role is not to provide an overall reaction plan follow-up solution, but merely the means to ensure a fast and efficient way for stakeholders to be more reactive and better informed.

4.1 Scenarios

As detailed in Work Package 3, the list of scenarios to be taken into account is detailed in the table below:

Table 8 – Scenario list

Scenario	Title
1	Cyber-physical attack targeting power supply of the hospital

2	Cyber-physical attack to steal patient data in the hospital
3	Cyber-physical attack targeting the population, IT systems and medical devices in the hospital, and patient data base
4	Cyber-physical attack targeting the air-cooling system of the hospital
5	Shooting, explosive or sabotage in critical places (visible or invisible)
6	Theft at hospital equipment, access to hospital network and IT systems
7	IOT medical wearable devices (outside / inside)
8	Distributed management over distributed buildings, considering external stakeholders (e.g., pharmacy, outpatients)
9	Cyber-physical attack to block national crisis management

These scenarios may be subject to changes.

Implementation phase will determine each scenario reaction plan. The methodology to be followed will help determine:

- Scenario path
- Related physical and cyber security incidents
- Related assets and impacts
- Response plan
  - Stakeholders & roles
  - Detailed step by step response plan (who gets what info, and what is expected from them)

4.2 Threat response in Greek hospitals

In this direction and in order to support the development of Response plans, the perspective and procedure that applies in Greece is presented hereafter (trying to be as generic as possible, giving the ability to be used in each use case), based on a set of Hospital internal and external security stakeholders.

Crisis management has been defined as "the developed capability of an organization to prepare for, anticipate, respond to and recover from crises (British Standard Institute (BSI), 2014). The full cycle of crisis management can be described in the following four phases: (a) **Preparedness,** (b) **Response,** (c) **Recovery and** (d) **Mitigation.** Threat response is a set of actions taken to stop the causes of an imminent hazard and/or mitigate the consequences of potentially destabilizing events or disruptions, and to recover to a normal situation (ISO 22300:2018)[1]. As undertaking and establishing an incident response effectively is complex, substantial planning and resources are required. It is important that healthcare organizations develop and implement a coordinated approach to threat response, where organization missions, business functions, strategies, goals, and objectives are considered. In the following paragraphs, we will analyze threat response process; the stakeholders involved; and the systems used.

[1] ISO 22300:2018 (en) - Security and resilience. https://www.iso.org/obp/ui/#iso:std:iso:22300:ed-2:v1:en

4.2.1 Legislative framework in Greek hospitals

Both generic and case specific laws, response plans and policies exist at a national level outlining basic incident response procedures and the establishment of necessary safety and security measures. These may refer to and include general or partial evacuation processes, security procedures application in order to protect the venue (e.g. emergency department, the triage area, other healthcare facilities, the morgue etc.) and other sensitive, critical or valuable assets and areas (e.g. computer room, central servers or blood bank, pharmacy etc.) from unauthorized access, implementation of operational procedures for securing premises perimeter by any unauthorized entry, deployment of entry and exit control measures, implementation of ambulance trafficking plan, enforcement of measures for the preservation of food, water and medical supplies and procedures for the protection of IT infrastructure, pharmacy and blood bank stockpile but also epidemiological monitoring and surveillance of infectious diseases processes, risk assessment and management of acute public health incidents, emergency intervention and management of an epidemic outbreak, or of an intentional or accidental release of biological or chemical agents.

The relative national and EU laws are the following:

- Organizational chart of the Ministry of Health (Presidential Decree 121 / 2017, Government Gazette 148 A ') & Law No.4486/2017 "Reform of Primary Healthcare, Emergency Regulations of the Ministry of Health and other provisions" (Government Gazette 115 A') – definition of National Health Operations Center (NAHOC)
- Law No.3329/2005 (Government Gazette 81 A ') – describes Hospital's General Manager duties
- Law No.3370/2005 (Government Gazette 176 A ') – describers epidemic outbreak management process
- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC
- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU
- eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century
- Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
- The Directive on security of network and information systems (NIS Directive)
- Regulation of The European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (''Cybersecurity Act'')

Moreover, to effectively and efficiently handle cyber and/or physical threats, an **incident response plan** is required, as it supports reporting of security breaches and compliance with security rules and allows organizations to identify, minimize the damage, and reduce the cost of a physical or cyber-attack, while finding and fixing the cause to prevent future attacks. The incident response plan should: (a) provide a roadmap for implementing its incident response, (b) support the accurate documentation of events, (c) identify contributing factors that led to the incident and steps that should be taken to prevent the recurrence of a similar incident, (e) be distributed to internal and external stakeholders, (f) be tested and (f) be evaluated and reviewed accordingly. Moreover, a response plan should include the following: (a) a cost benefit analysis for the most important assets in the hospital as it needs to be adequately protected, (b) a clear list of the most important assets (physical and cyber), (c) a security strategy for hospital key assets and a Bring Your Own Device (BYOD) and mobile device policy for all users, (d) an activity plan for training and awareness raising and (d) clear roles and responsibilities of incident response team and stakeholders involved. The response plans in Greece are the following:

- National General Plan of Civil Protection - XENOKRATIS (Ministerial Decision No.1299 / 10-04-2003, Ministry of Interior, Government Gazette 423 B),
- Emergency operations plan with code name PERSEUS which is a generic plan outlining basic incident response procedure (developed by NAHOC) and
- Emergency operations plan with code name SOSTRATOS which is a case specific plan of hospital evacuation procedures after an earthquake (developed by NAHOC).

These plans in combination with specific legal provisions lying under the national laws or after the transposition of the relevant European legislative framework into the national legal system designate specific individuals or in-hospital agencies, bodies or committees that have the mandate to fulfill all the tasks and responsibilities related to the hospital emergency planning and response strategy.

In addition, an **evacuation and patient transfer plan/process** should be defined. It manages the planning and assists a hospital in refining and augmenting its efforts to prepare for the possible evacuation of part or all of the facility. Moreover, hospital should have and follow **physical and cyber security policies** that can support preparedness, response, recovery and mitigation phases of crisis management.

4.2.2 Threat response stakeholders in Greek hospitals

In addition, organizations should consider the coordination and sharing of information with internal and external stakeholders, including, external service providers and organizations. Healthcare organizations' security stakeholders are individuals or organizations that may contribute to, be affected by, or get involved in issues related to security planning, response or recovery in any given emergency situation or posed threat. Security stakeholders can be categorized according to their involvement and perceived proximity to the healthcare organization into internal and external, as further analyzed below.

Internal stakeholders are these entities designated with duties and responsibilities within the organization's environment, play a role to its performance and can affect or can be affected by all the decisions made.

A comprehensive list is detailed hereafter:

- The Data Protection Officer's (DPO) primary role is to ensure that processing personal data of its staff, customers, providers, or any other individuals follows the applicable data protection rules.

- Physical Security manager / Security personnel main role is to develop and implement security policies, protocols and procedures, manage training of security officers and guards (internal and external), plan and coordinate security operations and staff when responding to alarms and emergencies, all related to the physical part of security.
- IT Security manager / Security personnel is responsible for leading and managing all the relevant activities of the Information Security Risk Assessment and Security Operations team (implementation, installation, monitoring and service/support of healthcare IT infrastructure such as networks, platforms, applications, devices etc., develop, assess, update and enforce security plans and policies in accordance with IT policies, standards, and compliance requirements, respond to cyberattacks and mitigate cyber risks, provide reports on security issues/threats and train the IT personnel).
- Technical Manager/ Technical staff is also stipulated as internal stakeholder. The technical staff not only can identify the sensible technical components for a health structure, such as energy, elevators, technical gas/fluid, temperature, air control systems or building management but also is responsible to manage physical access rights, hospital Scada systems, natural hazards and safety events to healthcare organizations infrastructures and processes.
- Security Officer is responsible manager for security and safety operations of the hospital. In case of a threat, the Security Officer assesses the criticality and activates and coordinates the Crisis Management Team (CMT).
- Security and safety teams are responsible for safeguarding the Hospital against physical attacks: (a) technical assets (e.g. gas, electricity, water), (b) hazardous materials (e.g. radioactive, diagnostic or therapeutic materials), (c) personnel and patients, (d) against natural disasters and fire- fighting. These teams are continuously trained and participate in tabletop and field exercises and simulations with patients, staff, fire brigade, volunteers etc.
- Crisis Management Team “focuses on detecting the early signs of a crisis; identifying the problem; preparation of a crisis management plan; encouraging the employees to face problems; and solving the crisis” (Mikušová, et al., 2019).

On the other hand, the **external stakeholders’** category includes individuals or groups outside the organization that can affect or can be affected by it, as they are conjoint into an interdependent relationship. These are described in the following paragraphs:

- Interconnected/Interdependent Critical Infrastructures and related Organizations include all types of CIs (as described in the EU Directive 114/2008, the NIS Directive and national policies, that are further analyzed in section 1.3 of this paper), Member States, National Authorities and EU officials related to CI resilience or Healthcare programs and regulatory work. These entities also support incident management for physical and cyber threats and respond against respective security events.
- Law Enforcement Agencies (LEAs) mission is to ensure peace and order as well as citizens’ unhindered social development which also includes general policing duties and to prevent and interdict crime.
- Fire Brigade provide fire, rescue and assistant services and deploys operational procedures during natural or man-made disasters (e.g. structured fires, technological

disasters, earthquakes, floods, chemical - biological - radiological - nuclear (CBRN) threats, etc.) also falls into this category.

- Emergency Medical Services (EMSs) refer to rescue and emergency services that provide medical response to injured or ill people at the scene of the accident.
- Other healthcare control centers identified through the interviews conducted are the following: (a) Centre for Disease Control and Prevention; (b) National Health Operations Centre (NHOC) and (c) Greek Atomic Energy Commission.
- General Secretariat for Civil Protection and Administrative regions of Greece is the body responsible for promoting the country's civil protection relations with relevant international organizations and relevant civil protection agencies in other countries.
- Ministry of Health role in crisis management process is to support, coordinate and formulate crisis management process in healthcare organizations.
- Hellenic National Defense General Staff (HNDGS) - Directorate of Cyber Defense is responsible for defending against acts of cyberwarfare, and for the coordination of cyber defense exercises (Hellenic National Defence General Staff, 2019)
- National Intelligence Service (EYP) is designated as National Authority against Electronic Attacks (national CERT), competent for preventing and statically and actively dealing with electronic attacks against communication networks, information storage facilities and computer systems (NIS, 2019).
- Telecommunications & Post Commission (EETT) is the national regulator for electronic communications (ENISA, 2019).
- ADAE is the Hellenic Authority for Communication Security and Privacy (ENISA, 2019).
- Hellenic Data Protection Authority is a Greek Authority responsible for the protection of personal data and privacy of individuals constitutes a fundamental human right. Data protection law grants the data subjects, i.e. individuals, certain rights and imposes certain responsibilities on data controllers, i.e. anyone who keeps personal data in a file and processes it (Data Protection Authority, 2019).

Table 9. Hospital's stakeholders involved in physical and cyber security crisis management process

	Hospital safety and security stakeholders	Cyber attacks	Physical attacks
Internal	1. Data Protection Officer	V	
	2. Physical Security manager / personnel		V
	3. IT Security manager / personnel	V	
	4. Technical Manager/ Technical staff	V	V
	5. Security Officer	V	V
	5. Security and safety teams		V
	6. Crisis Management Team	V	V
External	7. Interconnected Critical Infrastructures and related Organizations	V	V
	8. Law Enforcement Agencies	V	V
	9. Fire Brigade		V
	10. Emergency Medical Services (ambulance)		V
	11. Other healthcare control centers • Centre for Disease Control and Prevention • National Health Operations Centre • Greek Atomic Energy Commission		V

Hospital safety and security stakeholders	Cyber attacks	Physical attacks
12 General Secretariat for Civil Protection and Administrative regions of Greece	V	V
13. Ministry of Health	V	V
14. HNDGS - Directorate of Cyber Defense	V	
15 National Intelligence Service	V	V
16. EETT	V	
17. ADAE	V	
18. Hellenic Data Protection Authority	V	V

4.2.3 Threat response process in Greek hospitals

Response initiates when an incident is detected by an internal stakeholder with a manual or automated way. The Security Officer should immediately be notified and the information that will be used for the initial assessment of the incident should be gathered. Information gathering and assessment is a crucial and continuous step of this phase, as it highly depends not only on the source, quality, relevance of it, but also on the capacity of stakeholders involved in analyzing, interpreting, understanding and adding value to raw information.

Based on the criticality of the incident, the Security Officer should inform and trigger Crisis Management Team; Hellenic Police, Cyber-Crime division and/or National CERT, and the Hellenic Fire Services if needed, depending on the nature of the threat. Relative information (that can be used for management, informative purposes) should be communicated on-time, accurately and precisely to internal and external stakeholders, in order to manage crisis management process and protect the brand and reputation of the organization.

The Security Officer and CMT should cooperate with competent authorities (Hellenic Police/ Hellenic Fire Service) facilitating their work by providing any needed information or additional resources; as well as for search and rescue operations within the hospital premises. CMT should determine, plan and define which response plan(s) should be activated (e.g. ambulance trafficking plan, evacuation, business continuity etc.); resources should be allocated and released; and actions should be assigned and tracked. For example, they should:

- Cooperate with the traffic police on site, in order maintain the route free of any given obstacle. Traffic and pedestrian control teams are organized on site in cooperation with leas.
- General evacuation process - in the case that a general evacuation order is activated (supervised by the security personnel): (a) specific patient transfer teams are mobilized immediately to accompany the patients to pre- selected security areas, (b) the teams are made up of patient carriers and nurses and coordinated by clinicians or an experienced nurse coordinator, (c) the process is supervised by the security officer.
- An ambulance trafficking plan for arriving and leaving the hospital premises is implemented (an "airport type" scheme where ambulances and all vehicles arrive at one entry, disembark and leave form another exit). A secondary alternative ambulance route is also identified.

Other actions that might take place, depending on the criticality of the threat, are the following:

- Inform personnel to carry at all times their professional identification cards or other appropriate evidence so to ensure their entry and moving into the hospital and facilitate possible security controls.
- All entry and exit points are fully controlled by hospital security unit and can be locked or disabled /unlocked at all times upon request. Moreover, entry and exit control measures are applied.
- Establish a management station on site e.g. the ground floor of the hospital near the central entrance for all personnel to report for duty where responsibilities can be delegated from the appointed executives.
- Appropriate areas for victims' relatives & authorized visitors upon sop coordinator's request; and for media representatives upon sop coordinator's request are organized and secured.
- Immediate site and infrastructure protection measures are deployed depending on the nature of the incident (e.g. Activating the hospital's firefighting team) before the arrival of the competent authorities (Hellenic police/ Hellenic fire services) if needed.
- Security personnel ensure that the patients' personal belongings are carefully registered and secured.
- Secure the emergency department, the triage area, the healthcare facilities, the morgue and other sensitive or strategic areas or spaces (e.g. computer room, central servers or blood bank, pharmacy etc.) From unauthorized access.
- Food, water, medical supplies and blood bank inventories are secured.
- People from unauthorized areas are removed and evacuated areas are secured.
- The premises and the outpatient clinic are evacuated if needed from the chronic patients, escorts and visitors.
- For patients that there is an imperative medical reason to be hospitalized in the resuscitation section, supplementary space is created under the responsibility of the respective medical director.
- Cancelation of regular surgeries and interventions are accelerated.
- Manage patients exposed to CBRN factors - in the case of suspected exposure to biological / chemical agents, the hospital should be placed in an emergency situation, following the release of biological or chemical agents within its area of responsibility.
- Isolate infected victims - if this becomes necessary infected victims are accommodated in negative pressure units in the department of infectious diseases under the supervision of the infections control committee of the hospital.

They should also inform the on-call personnel and all human resources reserve as the deployment of the plan escalates with a suitable automated alert system integrated to the hospital's call center (e.g. Hospital's pagers, receiving SMS messages on mobile phones, audible alarm signals, special alarm device or system).

The afore-mentioned steps could repeat, till resources return to their original use and status (demobilization) and crisis terminates.

All taken actions and observations are documented and a report to the national data protection authority (if required) should be made and sent. Moreover, the National Health Operations Center of the Hellenic ministry of health should be notified for the current situation as the competent supervising health authority- it has also the responsibility to give status reports on a regular basis.

Finally, CMT should cooperate with Hellenic police / fire service to support the investigation of the event (if required).

4.2.4 Alert systems in Greece

In general, the communication and alerting between Organizations after a security incident is mainly done through manual telecommunication systems (e.g. telephone communication between the Command and Control center/Security Manager of a Hospital with Hellenic Police). In August 2019, Greece's General Secretariat for Civil Protection launched the single European emergency 112 phone number, which operates on a 24-hour basis, seven days a week and aims to warn residents and visitors of potential dangers, including wildfires. Currently in pilot phase operating out of two crisis management centers, the European emergency number program will run through to year's end via SMS messaging with authorities set to announce its full implementation – to also include Advanced Mobile Location (AML) technology to receive location information from mobile phones (already in application elsewhere in Europe) – in the coming period. At the same time, the Civil Protection authority will be launching an awareness-raising campaign on ways to link up via app to the warning HQs. Hundreds of visitors to Greece and locals received warning messages over the weekend in view of high risk of forest fires.

It should be noted that citizens and visitors can and should call (for free) 112 for help or in case of emergency as well as to report fires. The 112 number can be dialed for free in any EU country to contact emergency services. The Greek Digital Governance Minister confirmed that the "112" program will be finalized and in full application by the beginning of next year 2020, adding that once completed it will be able to send messages to all phones. Currently, the system cannot offer Cell Broadcast – i.e. sending messages to multiple mobile telephone users in a defined area at the same time.

4.2.5 Requirements for existing and future systems, process

Key competences to detect, evaluate, notify, and respond promptly and effectively in real time to any given threat should be accurately defined. Minimum core capacities include areas such as emergency coordination centers establishment at all levels of operation (tactical, operational and strategic), emergency plans deployment, effective surveillance systems installation, preparedness and response procedures execution, crisis communication strategy formation, human resources mobilization policy initiation, laboratory networking disposition. In addition, a threat response system should have at least the following requirements:

- Fast response (physical and cyber).
- Clear emergency process for CBRN Incidents.
- Clear emergency process for a fire incident.
- Clear emergency response process for a physical (theft, sabotage, etc.) attack.
- Clear emergency response process for a cyber-attack.
- Clear evacuation plan.
- Clear patient transfer to other health facilities process.
- A business continuity plan to take place.

- System to warn the entire hospital immediately (e.g. text to specific mobile phones, messages in displays, sound alarms).
- Communication (e.g. automatic optimized call handling) with LEAs and EMS providing on-time, accurate and precise information on hospital suspicious behavior, threats and events
- Communication with health/emergency management authorities and other hospitals providing on-time, accurate and precise information on event, patient's personal and medical details (in case of patient transport)
- High level of maturity is mandatory for a high acceptance level.
- A key mapping feature is the display of what, where and when has happened
- Record provenance of data.
- Preserve audit trail (logs) of information used for decision making in order to improve future incident handling and to respond to legal challenge.
- Capture incidents that can be replayed for training purposes.

Given the fact that the current socioeconomic, physical and political environment's emerging hazards are of high complexity, the approach to improving the capacity of risk assessment and impact mitigation to any given physical or cyber threat should, therefore, be comprehensive, cross-sectoral and cross-border. In order, however, to propose a framework for improving and developing interoperability and interdisciplinary cooperation one should take into account existing and future possibilities of developing common operational processes and technologies in order to establish continuous and unhindered communication between first responders (e.g. LEAs, Fire Brigade, Medical Emergency Services) facilitating the necessary field coordination and ensuring timely and adequate response.

Even more importantly future endeavors should develop and enhance further internal cooperation among all existing emergency managing agencies involved at an operational or even strategic level (e.g. Civil Protection's Integrated Operational and Coordination Center or National Health Operations Center etc). But effective communication and coordination action plans are not possible unless common identifiable processes, mutually compatible technologies and contiguous emergency preparedness and response mechanisms are established.

In the future, improving the "one button police alert system" many banks or shops have, the hospital's control center might be able to send a computerized alert system with initial valuable information to cope with the incident (e.g. inform that a CBRN incident has happened in order for the responders to be equipped with respective PPE) for example in case of (1) active shooter incident; (2) hostage situation; (3) detonation of an IED; (4) fire, to be delivered to police emergency center (tel code "100" in Greece) or fire service emergency center (tel code "166" in Greece). The same system might be able to automatically transmit an SMS message or a message through a specific mobile application, to all personnel working at the hospital alerting them to "shelter-in-place" until further "all clear" message is sent. The SMS might be accompanied by a second message with directives on what to do (i.e. lock/fortify door; kill the lights; hide by a concrete wall; stay away from glass surfaces).

4.3 FMI's expectations in terms of reaction plan

For Police forces, in case of aggression or attack in a hospital, the time of reaction is crucial, so they need to be alerted as soon as possible to insure a rapid intervention. But, first, the hospital security practitioners will need to perform a verification before contacting the Police. The Safecare project aims to centralize all information needed to take the right decision, and it would help the security practitioners in phase of investigation, and it could accelerate the alert. The intervention protocols might be very strict depending on national regulation.

In France, citizens use the emergency telephone number "17" "Police-Secours" to alert an event. The call is received at the information and command center (CIC) of the Departmental Directorate of Public Security (DDSP). CIC will coordinate the intervention as soon as possible by sending one or multiple mobile police forces.

It is interesting to note that an automatic system of communication exists between the French Police and telemonitoring security company. This system called Ramses Evolution II is also dedicated to centralizing the alarm reception of sensible site which depend on the French Ministry of Interior. Other sites of the public French administration can also demand the connection to this system. So, a study to connect the Safecare platform and then the hospitals would be conduct.

In all cases, even though the alarm is raised by phone, the police will need to be informed of the evolution of the situation in central. This is very important to adapt the force engagement into the operation. It is also important to recall that the citizens, witness of the aggression, will also call the Police with a different point of view. So, for a better understanding of the situation, the police would request the postponement of the images of the video surveillance system of the hospital. But the Police will need to have contextualization the images with the nature of the place, and maps of the situation where the event occurs.

(A detailed nature of the force engagement is developed in D3.4).

5 Interconnection with SafeCare ecosystem

This section will cover the technical part of the communications between TRAS and its environment.

5.1 Data flows overview

Figure 3 of the “D6.2 *Specification about data exchange layer* “ describes how TRAS component interacts with its ecosystem. Below is a copy of the sequence diagram with few modifications, followed by its explanation.

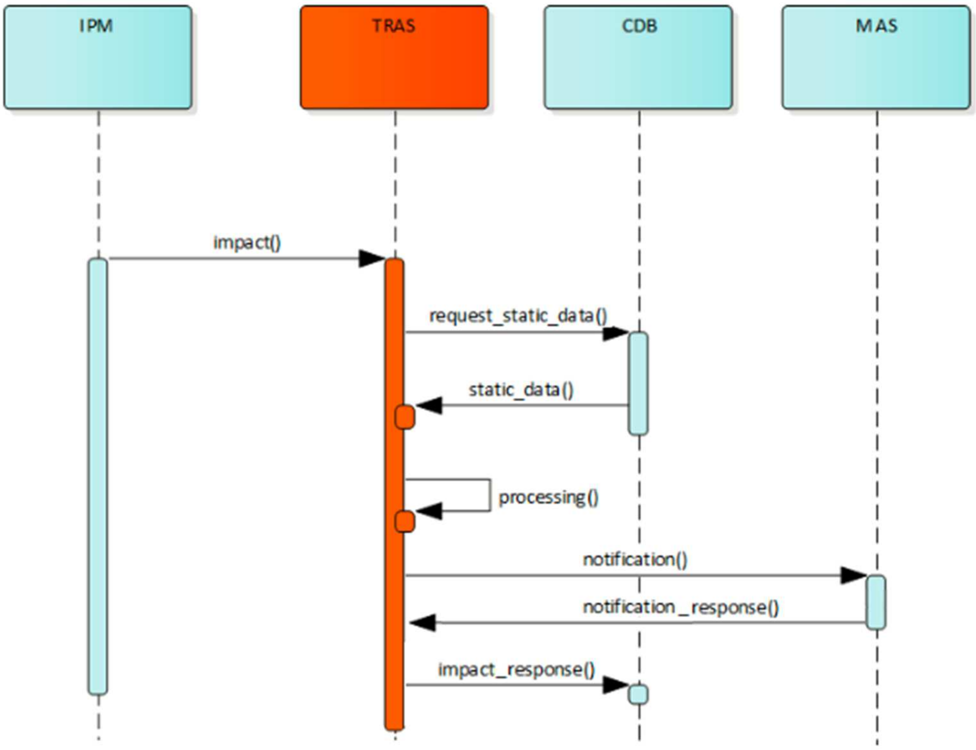

Figure 8 – Sequence diagram of data flow relating to TRAS

All starts with a Propagation Impact message published by IPM module and received by TRAS.

In order to process this message, the static data (containing asset definition) will be read from CDB (a local copy will also be available on TRAS).

Then the message can be properly processed, and the response plan launched accordingly. As part of the response plan, the stakeholders could be notified on their mobile application via the MAS module and their response saved.

Finally, a Propagation Impact Response will be generated as a campaign report and will be stored in the CDB.

All communications of dynamic data will be dealt through the DXL component using MQTT protocol.

The query and retrieval of static data from CDB will be performed without going through DXL using HTTP protocol via REST API.

5.2 Communication with Data Exchange layer (DXL)

- Communication protocol

As described in section 5 of deliverable D6.2, the MQTT (Message Queuing Telemetry Transport) protocol will be used for communication in between components. This will be possible thanks to DXL MQTT broker, acting as the intermediary for transactions of messages in between the publisher and the subscriber(s).

It is important to note that two different versions of this protocol are available:

- MQTT 3.1.1, ISO standardized, considered as a proven solution.
- MQTT 5.0, recently released in 2017, this version implements new features.

To ensure protocol compatibility, the broker (DXL) and the clients (publishers and subscribers) should be using the same protocol version, namely v3.1.1.

- Format of messages

Deliverable D6.2 proposes the JSON format to be used for messages exchanged via DXL. In order to parse successfully the JSON messages, their structure will have to be pre-agreed between the publisher and the subscriber(s). The next section proposes the JSON structures for the messages that TRAS module is involved with.

5.3 Communication with Impact Propagation Model (IPM)

TRAS will be subscriber of impact messages published by IPM.

Then, as soon as the message is published, TRAS should receive the message under JSON format.

Section 5.2.2 from D6.2 Specification proposes the following structure for JSON format:

```
{
        "impact_id":"XXXXXXX",
        "incident_id":"YYYYYYY",
        "assets":[
                {
                        "asset_id":"AAAAAAA",
                        "risk_type":"Fire",
                        "impact_score":1
                },
                {
                        "asset_id":"AAAAAAB",
                        "risk_type":"Fire",
                        "impact_score":0.8
                },
                {
                        "asset_id":"AAAAAAC",
                              "risk_type":"Data leak",

                              "impact_score":0.6

                    }

          ]

}
```

The message above could be translated in the real world as the following:

“This is an impact message with identification XXXXXXX, it has been generated from an incident with identification YYYYYYY. This impact could threaten the following assets of the hospital:

Asset AAAAAAA with a risk of Fire of a score of 1

Asset AAAAAAB with a risk of Fire of a score of 0.8

Asset AAAAAAC with a risk of Fire of a score of 0.6”

5.4 Communication with Mobile Alert System (MAS)

This section describes the two-ways communication between TRAS and MAS.

5.4.1 Notification publication

TRAS will be publisher of notification messages for MAS.

We propose that one notification message should be published for each recipient of the alert campaign, since each notification_response should be managed separately. The format of the message should be a JSON file as follows:

```
{
          Message_id: “ABCDEF”,

          impact_id:"XXXXXXX",

          incident_id:"YYYYYYY",

          timeout: (most likely a timestamp),
          from: (sender name as string),
          to: (end recipient address),
          message: (text message to be displayed)
          delivery_method: “confirmation required”
}
```

The *delivery_method* parameter could have different values:

- **“notification”** (Simple message delivery with no expected user feedback);

- **“acknowledgement required”** (Message delivery with explicit user acknowledgement expected. Falls back to “no answer” state after timeout);
- **“confirmation required”** (Critical message delivery with user accept/reject status expected. Falls back to “no answer” state after timeout).

5.4.2 Notification response publication

TRAS will be subscriber of the notification response messages published by MAS.

We propose that at least one notification response message should be published for each notification message.

In the case where the notification message is asking the recipient for reading acknowledgement and commitment for action, two notification responses could be sent, one “acknowledged” and one “confirmed” status.

A JSON message for notification response could look like the following. This is an example of a notification response message stating that the notification has been delivered and read:

```
{
        notification_response_id:”WWWWWWW1”,
        notification_id:”WWWWWWW”,
        impact_id:"XXXXXXX",
        incident_id:"YYYYYYY",
        timestamp: (last status time),
        delivery_status: “acknowledged”
}
```

The *delivery_status* parameter could have different values:

- **“acknowledged”** (user acknowledgement for message delivery);
- **“confirmed”** (user acceptation of commitment);
- **“rejected”** (user rejection of commitment).

5.5 Threat Response data format (for storage in CDB)

As stated in section 5.2.2 of D6.2, once the response plan is completed, a response message will be published as a report of the campaign of communication.

The purpose of this message is to be archived in the CDB for history review.

CDB will be a subscriber for the response topic.

This is an example of response message that could be published by TRAS. In this sample a call campaign has been performed on three recipients. All of them have replied but only one positively. The quorum policy was set-up to 100% of the recipients and thus has not been reached.

```
{
    "response_id":"0000000",
    "originate_impact_id":"XXXXXXX",
    "timestamp":1567432951,
    "response_status":"executed and accepted",
    "communication_details": {
        "template": {
         "name": "call",
         "id": "984a79bd635fcb032d3bf0",
         "config": {
          "recipients": {
           "source": "field",
           "value": "@recipients",
           "medias": [
            "personal",
            "professional",
            "mobile"
           ]
          },
          "quorum_policy": {
           "method": "rate",
           "value": 100
          },
          "retry_policy": {
           "maximum": 3,
           "delay": 60,
           "feedbacks": [
            "unknown"
           ]
          },
  "blocking": true,
  "template": {
   "id": "df160101-710c-4be6-9a18-0b4fc782e476",
   "draft": false
  }
 },
 "timeout": 10800,
 "topics": [],
 "title": "Campagne d'appels"
},
"id": "9c53d2d5-cabf-4bf0-ae8d-28622427ef0e",
"start": "2019-10-17T09:35:50.125000+00:00",
"end": "2019-10-17T09:36:42.648000+00:00",
"state": "finished",
"reporting": {
 "quorum": {
  "reached": false,
  "expected": 3,
  "progress": 1
 },
 "feedbacks": {
  "expected": 3,
  "progress": 3,
  "received": {
   "positive": 1,
   "negative": 2,
   "unknown": 0
  },
  "failed": 0
 },
 "contacts": [
  {
   "uid": "73hFaL0OODJAforMuJzEFJ",
 "external": false,
 "display_name": "Jean-Pierre Facque",
 "start": "2019-10-17T09:35:50.125119+00:00",
 "end": "2019-10-17T09:36:33.381040+00:00",
 "feedback": "negative",
 "attempts": 1,
 "calls": [
  {
   "uid": "702bcc10",
   "media": "mobile",
   "number": "+33xxxxxxxx",
   "attempt": 1,
   "feedback": "negative",
   "status": "completed",
   "workflow": "f6ab92eb-f34e-4550-87ad-261104a75f59",
   "start": "2019-10-17T09:35:50.326957+00:00",
   "end": "2019-10-17T09:36:33.380436+00:00"
  }
 ]
},
{
 "uid": "2FQsFeXBCBTtC1y49ypu7W",
 "external": false,
 "display_name": "David Fermet",
 "start": "2019-10-17T09:35:50.125119+00:00",
 "end": "2019-10-17T09:36:42.648143+00:00",
 "feedback": "negative",
 "attempts": 1,
 "calls": [
  {
   "uid": "c4e24de0",
   "media": "mobile",
   "number": "+33xxxxxxxx",
          "attempt": 1,
          "feedback": "negative",
          "status": "completed",
          "workflow": "c8221599-27e2-4efb-b31f-1eb58281c476",
          "start": "2019-10-17T09:35:50.457911+00:00",
          "end": "2019-10-17T09:36:42.647646+00:00"
        }
      ]
    },
    {
      "uid": "4Fo52KcW0zb4CucyS2et2e",
      "external": false,
      "display_name": "Christophe Le Dantec",
      "start": "2019-10-17T09:35:50.125119+00:00",
      "end": "2019-10-17T09:36:24.880801+00:00",
      "feedback": "positive",
      "attempts": 1,
      "calls": [
        {
          "uid": "dca7508a",
          "media": "professional",
          "number": "+33xxxxxxxx",
          "attempt": 1,
          "feedback": "positive",
          "status": "completed",
          "workflow": "06ae4551-a2a0-4892-9d5d-c729e45bd0f8",
          "start": "2019-10-17T09:35:50.671281+00:00",
          "end": "2019-10-17T09:36:24.880080+00:00"
        }
      ]
    }
  ]
}
```

```
                    }
}
```

6 Conclusion

In the SAFECARE global solution, TRAS will be in charge of providing the means to a faster and more efficient alert delivery. The implementation phase is key to reach the objectives and provide a measurement of the KPIs as specified in the DOA.

Next significant steps are:

- Test phase in Porto: to validate the integration with other SAFECARE components;
- IPM output and its association to hospital's reaction plans is the functional cornerstone of a successful alert delivery method and will be realized during the implementation phase;
- Detailed reaction plan specification with all related stakeholders.

This document intends to provide all functional aspects of TRAS and a project methodology (§3.3) for implementation phase at Marseille, Turin & Amsterdam, in order to reach the expected objectives of the SAFECARE project.

Implementation phase need to coordinate efforts of CNAM and ENOVACOM since our respective scopes of work have a strong common ground. As outlined in D6.6, listing assets and determining the ontology is made under the scope of related risks and reactions plans. The interview method could be adapted to be merged in a common methodology so as to be more efficient and focus each hospital involvement.

7 References

Arroues Pierre, Aulanier Romain, Boissart Marielle, Brasseur Anthony, Canalis Romain, Dali-Youcef Angèle, Gourain Marie, Rincourt Stéphanie, Sejourne-Talmard Adeline, Targhette Renan. 2018. *Conceptualiser la gestion d'une Situation Sanitaire Exceptionnelle dans le cadre d'un Groupement Hospitalier de Territoire.* s.l. : EHESP - Module interprofessionnel de santé publique, 2018.

British Standard Institute (BSI). 2014. *BS11200: Crisis Management – guidance and good practice .* s.l. : BSI, 2014.

CCS. *D6.1 Specification of the global architecture.* s.l. : Safecare document.

CNAM. *D6.6 Specitification of Impact and Decision Support Model.* s.l. : Safecare Document.

CSI. *D6.2 - Specification about data exchange layer.* s.l. : Safecare document.

Data Protection Authority. 2019. Data Protection Authority. [En ligne] 2019. https://www.dpa.gr/portal/page?_pageid=33,40911&_dad=portal&_schema=PORTAL.

DGS, DGOS. 2019. *Guide d'aide à la préparation et à la gestion des tensions hospitalières et des situations sanitaires exceptionnelles.* s.l. : Ministère de la Santé, 2019.

ENISA. 2019. Greek National Cyber Security Strategy. [En ligne] 2019. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view.

Hellenic National Defence General Staff. 2019. Hellenic National Defence General Staff. [En ligne] 2019. http://www.geetha.mil.gr/en/hndgs-en/history-en.html.

KEMEA. *Focus Group Bucharest - Scenario of Threat.* s.l. : Safecare document.

Mikušová, M. et P., Horváthová. 2019. Prepared for a crisis? Basicelements of crisis management in an organisation. 2019, Vol. 32, 1, pp. 1844-1868.

Ministère de la Santé. 2017. *Guide d'aide à l'élaboration d'un Plan de Sécurisation d'Etablissement (PSE).* 2017.

NIS. 2019. NIS. [En ligne] 2019. http://www.nis.gr/portal/page/portal/NIS/.