7SHIELD

SOLUTIONS FOR PROTECTING THE SPACE GROUND SEGMENTS: FROM RISK ASSESSMENT TO EMERGENCY RESPONSE

__Ilias Gkotsis__, Leonidas Perlepes, Aggelos Aggelis, Katerina Valouma, Antonis Kostaridis (SATWAYS)
Eftichia Georgiou, Nikolaos Lalazisis, Vasiliki Mantzana (KEMEA)

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under the grant agreement No 883284.

CPS4CIP 2022, 30 Sept 2022

Project Overview

- **7SHIELD** - ‘Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats’
- Funded by the EU Horizon 2020 programme in response to SU-INFRA01-2018-2019-2020 “Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe”
- Duration: 1 September 2020 – 28 February 2023(30 months)
- Coordinator: Engineering Ingegneria Informatica SpA
- EU funding: € 6,969,568.75

RUSSIA
FINLAND
IRELAND
GERMANY
POLAND
BELARUS
UKRAINE
FRANCE
ITALY
ROMANIA
SPAIN
PORTUGAL
TURKEY
MOROCCO
ALGERIA
TUNISIA

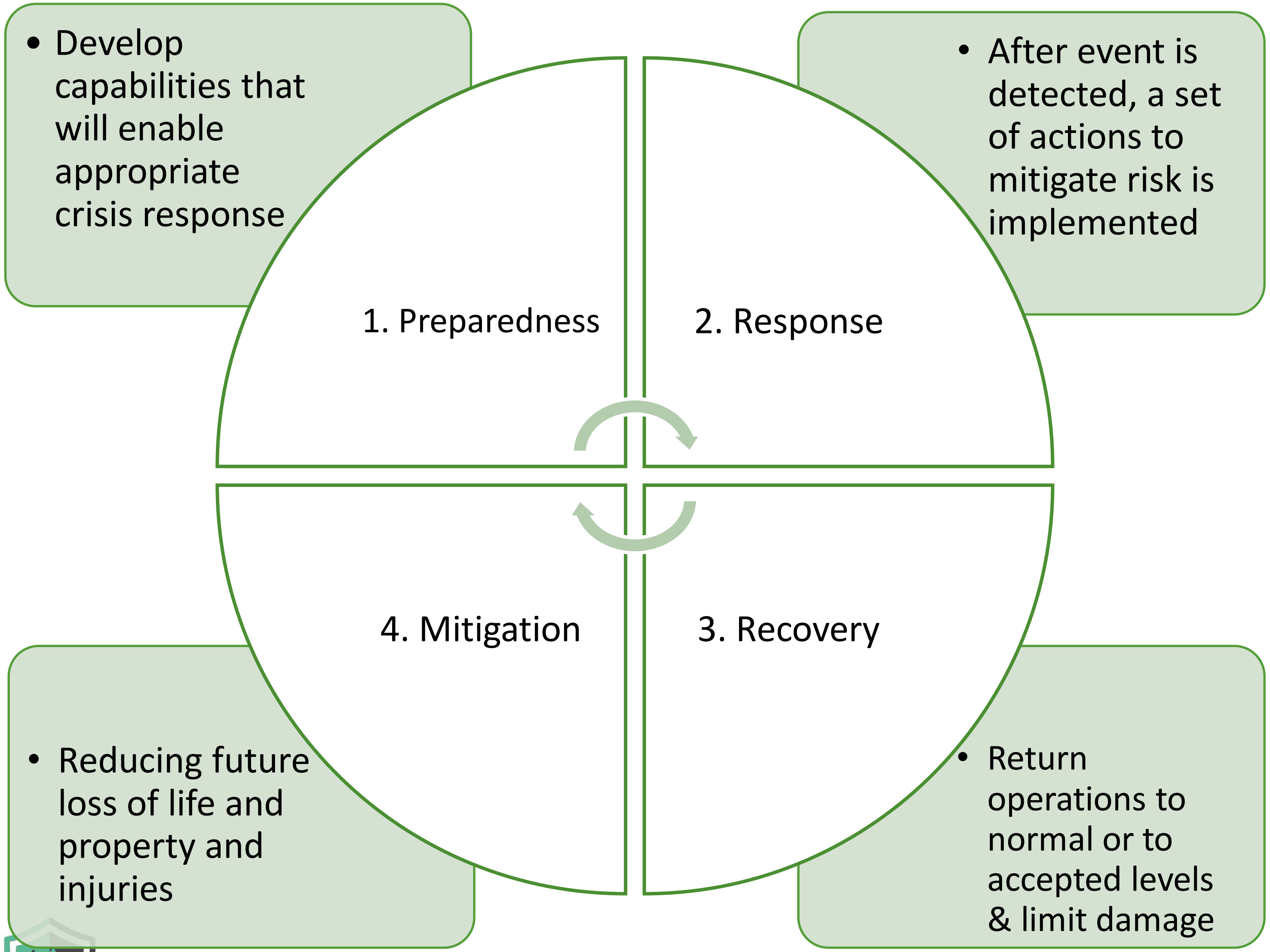
- 22 Partners from 12 European countries including
  - ✓ 5 GSSS infrastructure owners and operators (FMI, NOA, SPACEAPPS, DEIMOS, SERCO)
  - ✓ first responders organizations (EETT, HP, KEMEA)
  - ✓ academic/research institutes (CERTH, CENTRIC, CeRICT)
  - ✓ industry and technical SMEs (ENG, CS, INOV, STWS, DES, DFSL, RG, ACCELI, RESIL, CLS, CSNov)

GSSS main threats and security issues

- Facilities are **open to visitors**; thus, access is possible to unauthorized individuals with potentially abnormal or malicious intent (e.g. espionage, vandalism, terrorist or activist attack)
- Several facilities are **established in isolated areas** (e.g. forest, hills, etc.), and are unattended, which fact can be exploited by potential intruders/attackers
- GSSS are open air facilities, that are **exposed to UAV attacks**
- The **data centers** and the **satellite antennas** are some of the most important assets, that the services of the GSSS rely on. These assets are prone to both **physical and cyber threats** such as:
    - Unauthorized access to virtual machine/data
    - Unavailability of user services due to DDoS.
    - Unauthorized access and Damage to the server/data room
    - Sniffing attack (e.g. sniff the user authentication traffic between a client and a serve, trying to extract password hashes or authentication information)
    - Ransomware attack
    - Natural hazards
    - Interruption/Disruption of power supply, communication etc. or theft of critical equipment

*GSSS: Ground Segments of Space Systems

Crisis management and Security solutions



- Develop capabilities that will enable appropriate crisis response

- After event is detected, a set of actions to mitigate risk is implemented

- Reducing future loss of life and property and injuries

- Return operations to normal or to accepted levels & limit damage

Physical security

- ✓ Perimeter protection,
- ✓ Guards,
- ✓ Building management,
- ✓ Intrusion detection and access control,
- ✓ Video surveillance (including video analytics),
- ✓ Audio surveillance,
- ✓ CBRNe sensors,
- ✓ Physical Security Information Management (PSIM) systems,
- ✓ Fire detection and alarm system,
- ✓ UAV and Counter-UAV systems,
- ✓ LIDAR and Radar systems with innovative detection algorithms.

Cyber security

✓Data Protection,

✓ Network Monitoring,

✓Intrusion Detection and Response Systems,

✓ Endpoint Monitoring,

✓ Digital Authentication and Access Control,

✓Software Development based on privacy by design techniques,

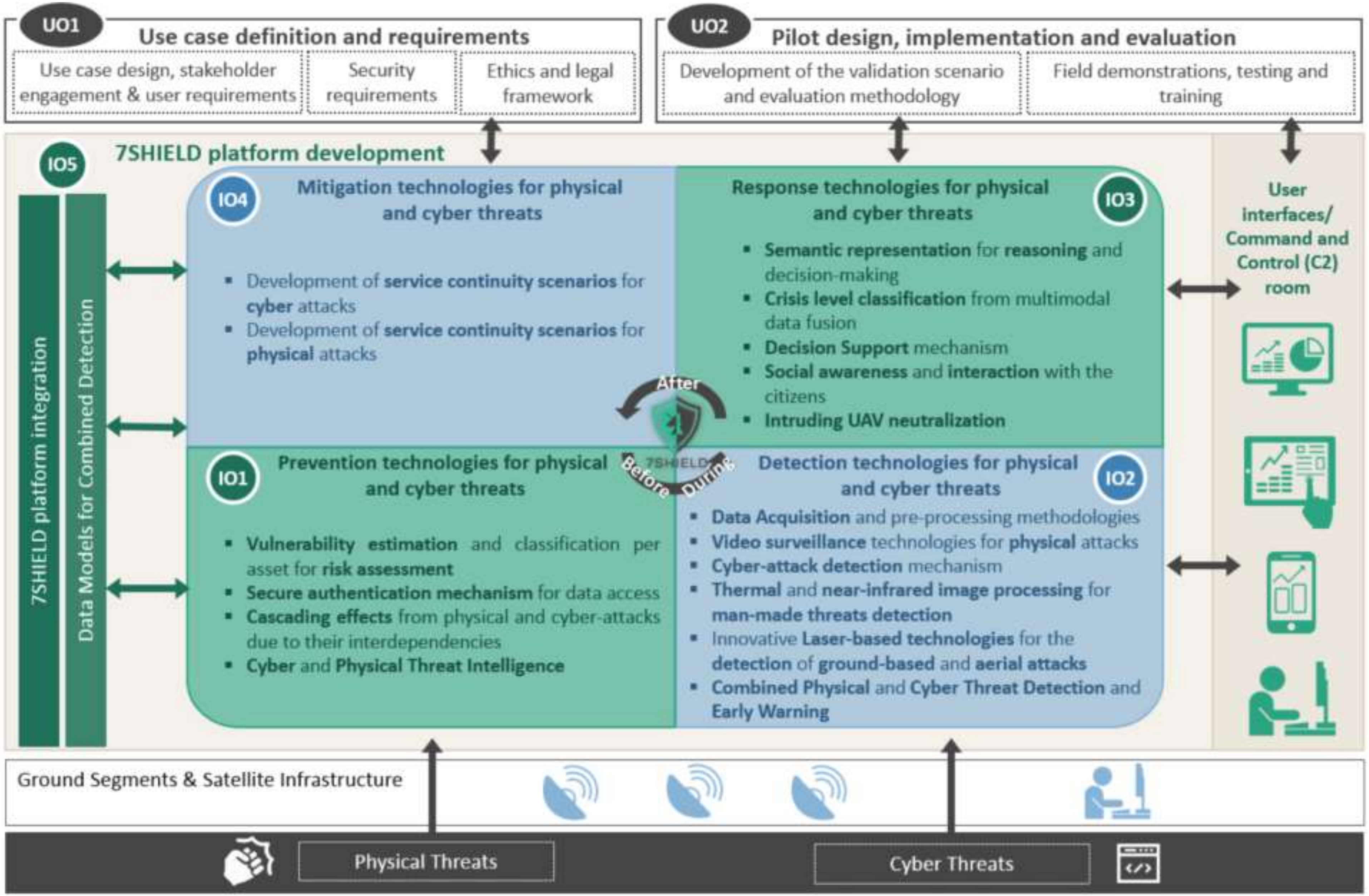
✓IoT Sensors,

✓ Artificial Intelligence techniques,

✓Event recording and audit systems,

✓Secure remote access.

7SHIELD project organization



UO1 Use case definition and requirements
- Use case design, stakeholder engagement & user requirements
- Security requirements
- Ethics and legal framework

UO2 Pilot design, implementation and evaluation
- Development of the validation scenario and evaluation methodology
- Field demonstrations, testing and training

IO5 7SHIELD platform development

7SHIELD platform integration

Data Models for Combined Detection

IO4 Mitigation technologies for physical and cyber threats
- Development of **service continuity scenarios** for **cyber** attacks
- Development of **service continuity scenarios** for **physical** attacks

IO3 Response technologies for physical and cyber threats
- **Semantic representation** for **reasoning** and decision-making
- **Crisis level classification** from multimodal data fusion
- **Decision Support** mechanism
- **Social awareness** and **interaction** with the citizens
- **Intruding UAV neutralization**

After

7SHIELD

Before

During

IO1 Prevention technologies for physical and cyber threats
- **Vulnerability estimation** and classification per asset for **risk assessment**
- **Secure authentication mechanism** for data access
- **Cascading effects** from physical and cyber-attacks due to their interdependencies
- **Cyber** and **Physical Threat Intelligence**

IO2 Detection technologies for physical and cyber threats
- **Data Acquisition** and pre-processing methodologies
- **Video surveillance** technologies for **physical** attacks
- **Cyber-attack detection** mechanism
- **Thermal** and **near-infrared image processing** for **man-made threats detection**
- Innovative **Laser-based technologies** for the **detection** of **ground-based** and **aerial attacks**
- **Combined Physical** and **Cyber Threat Detection** and **Early Warning**

User interfaces/ Command and Control (C2) room

Ground Segments & Satellite Infrastructure

Physical Threats

Cyber Threats

Arctic Space Centre in Finland

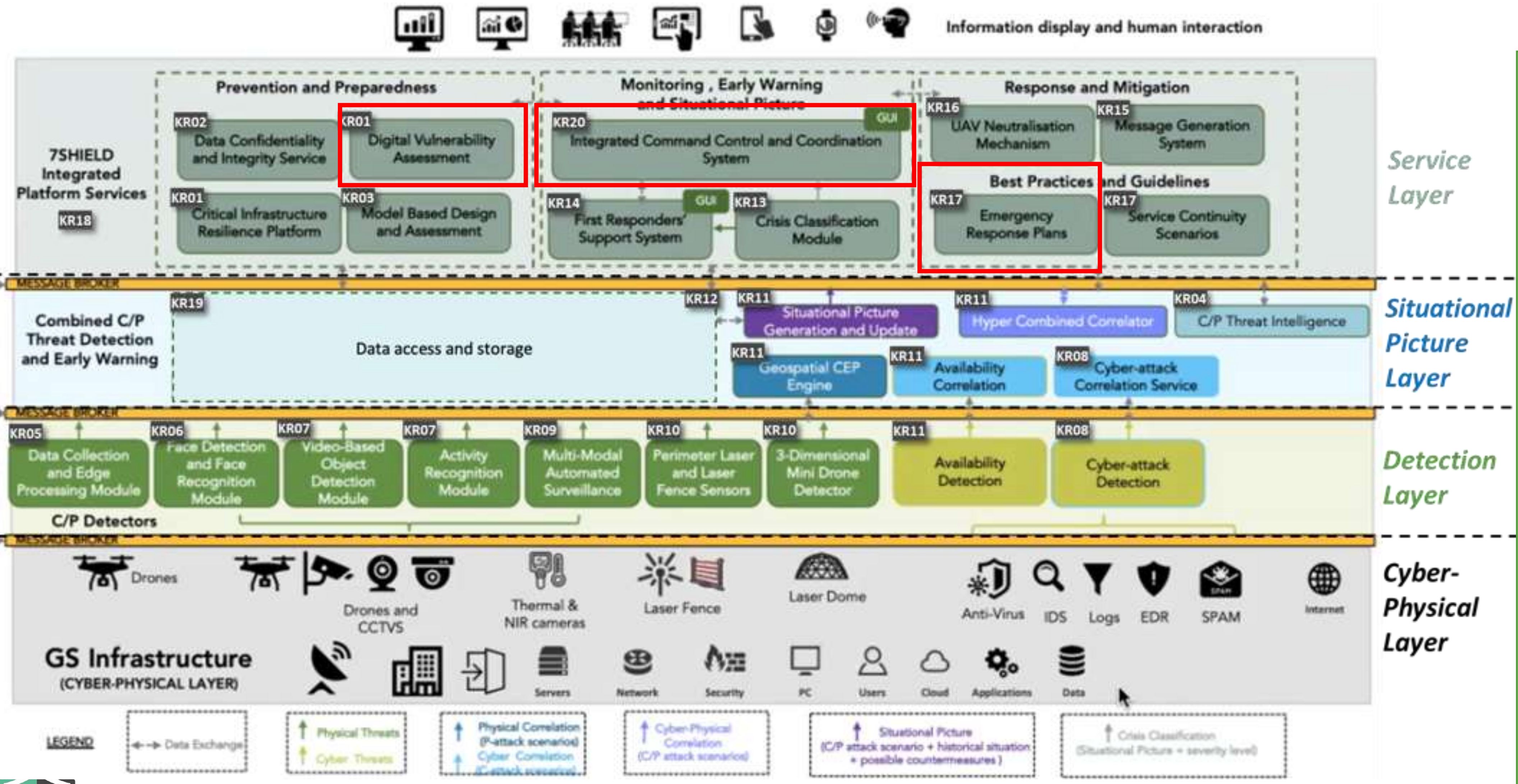
ICE Cubes Service in Brussels

Deimos Ground Segment in Spain

Ground Segment of NOA in Greece

ONDA DIAS platform in Italy

7SHIELD conceptual approach



Information display and human interaction

7SHIELD Integrated Platform Services

KR18

Prevention and Preparedness

KR02 Data Confidentiality and Integrity Service

KR01 Digital Vulnerability Assessment

KR01 Critical Infrastructure Resilience Platform

KR03 Model Based Design and Assessment

Monitoring , Early Warning and Situational Picture

GUI

KR20 Integrated Command Control and Coordination System

GUI

KR14 First Responders' Support System

KR13 Crisis Classification Module

Response and Mitigation

KR16 UAV Neutralisation Mechanism

KR15 Message Generation System

Best Practices and Guidelines

KR17 Emergency Response Plans

KR17 Service Continuity Scenarios

Service Layer

MESSAGE BROKER

Combined C/P Threat Detection and Early Warning

KR19

Data access and storage

KR12

KR11 Situational Picture Generation and Update

KR11 Hyper Combined Correlator

KR04 C/P Threat Intelligence

KR11 Geospatial CEP Engine

KR11 Availability Correlation

KR08 Cyber-attack Correlation Service

Situational Picture Layer

MESSAGE BROKER

KR05 Data Collection and Edge Processing Module

KR06 Face Detection and Face Recognition Module

KR07 Video-Based Object Detection Module

KR07 Activity Recognition Module

KR09 Multi-Modal Automated Surveillance

KR10 Perimeter Laser and Laser Fence Sensors

KR10 3-Dimensional Mini Drone Detector

KR11 Availability Detection

KR08 Cyber-attack Detection

C/P Detectors

Detection Layer

MESSAGE BROKER

Drones

Drones and CCTVS

Thermal & NIR cameras

Laser Fence

Laser Dome

Anti-Virus

IDS

Logs

EDR

SPAM

Internet

GS Infrastructure

(CYBER-PHYSICAL LAYER)

Servers

Network

Security

PC

Users

Cloud

Applications

Data

Cyber-Physical Layer

LEGEND

Data Exchange

Physical Threats

Cyber Threats

Physical Correlation (P-attack scenarios)

Cyber Correlation (C-attack scenarios)

Cyber-Physical Correlation (C/P attack scenarios)

Situational Picture (C/P attack scenario + historical situation + possible countermeasures)

Crisis Classification (Situational Picture + severity level)

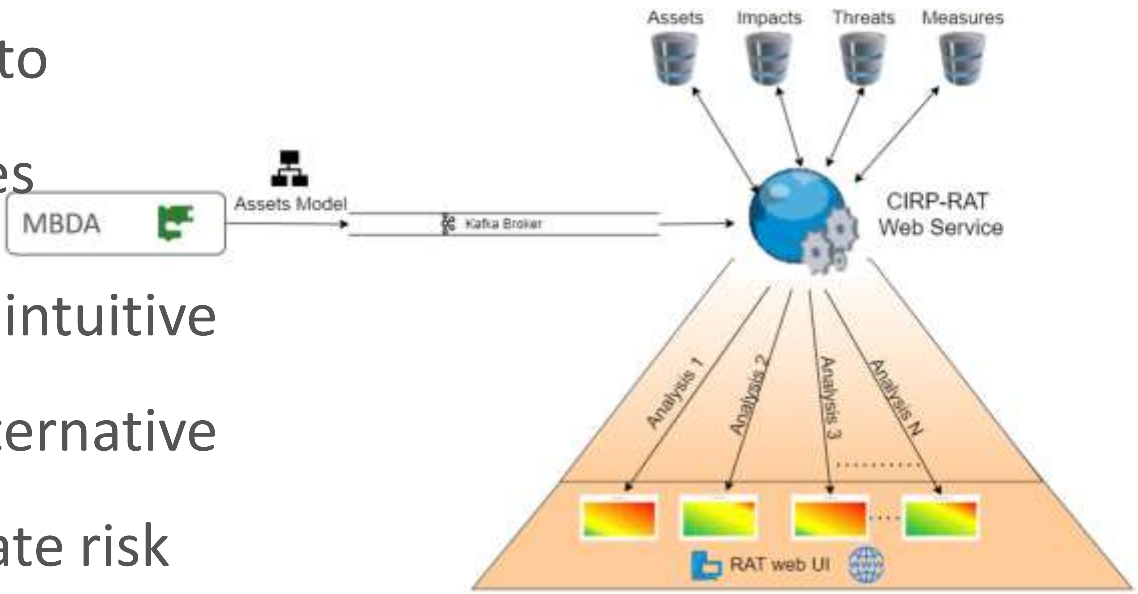
Main solutions for Operators:

- ✓ **Risk Assessment tools**
- ✓ Data Confidentiality and Integrity
- ✓ Interdependencies and cascading effects
- ✓ **Integrated C3 System**
- ✓ Decision Support System
- ✓ Crisis Classification Tool
- ✓ Social Awareness and Warning Message
- ✓ Service Continuity Scenarios
- ✓ **Emergency Response Plans**

7SHIELD

CIRP Risk Assessment Tool

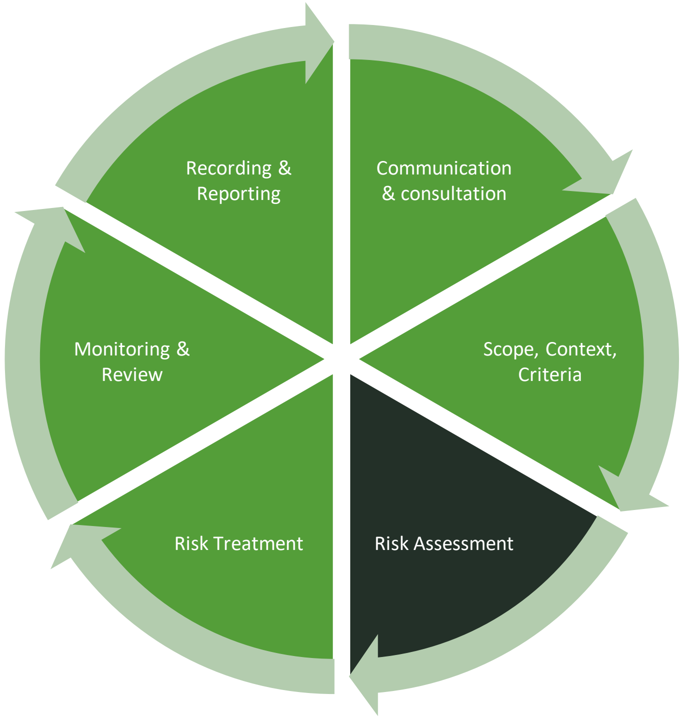
- CIRP-RAT is designed as an extension of the CIRP (Critical Infrastructure Resilience Platform) provided by Satways. CIRP is an end-to-end modelling component, able to provide online and offline simulation functionalities

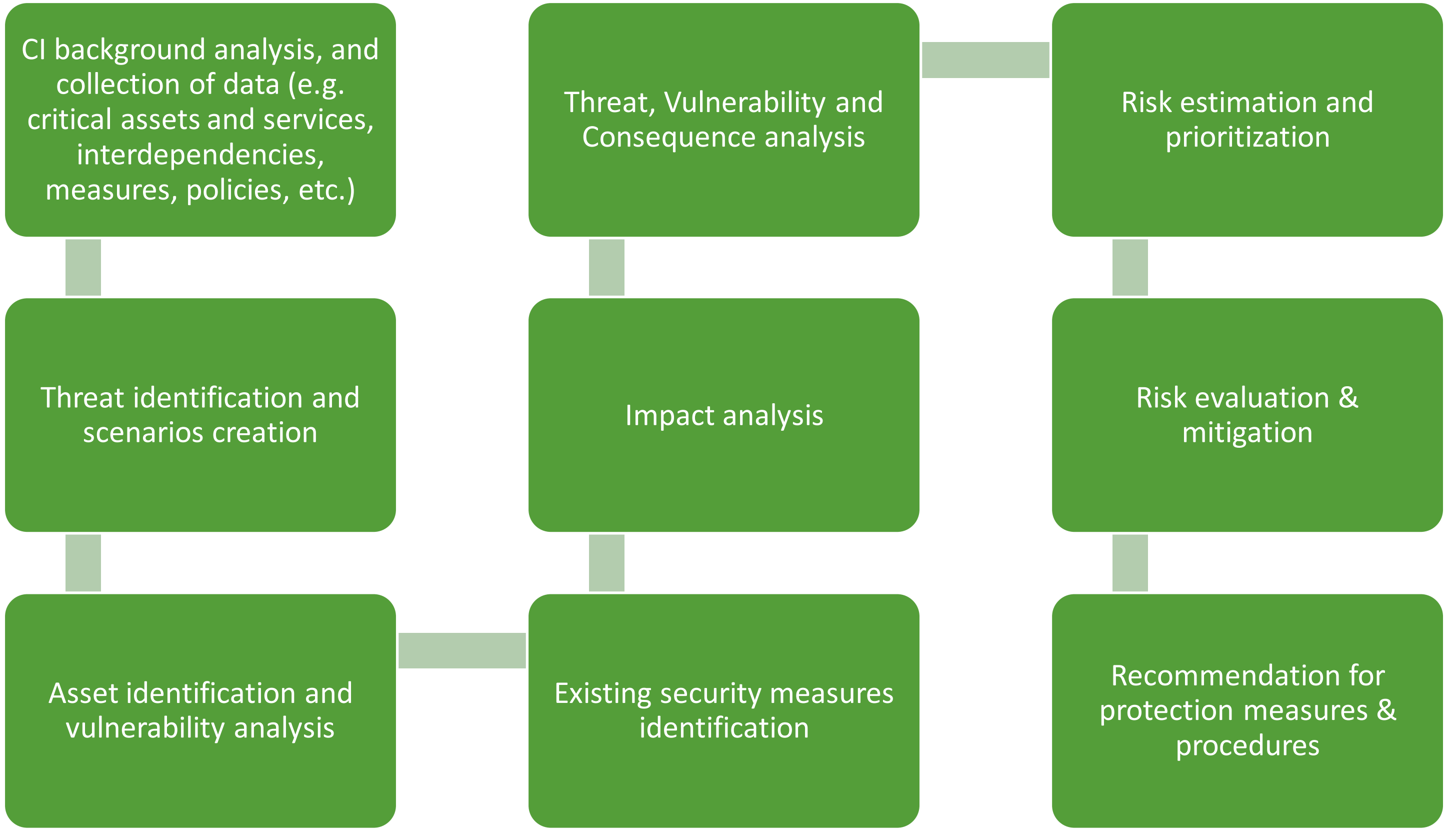


- CIRP-RAT, is a web-based tool, offering through an intuitive and user-friendly interface the capability to run alternative what-if scenarios (assessments), in order to calculate risk and to identify adequate response options

7SHIELD Risk assessment process

CIRP-RAT provides the CI operator with risk assessment information in a stepwise process:





CI background analysis, and collection of data (e.g. critical assets and services, interdependencies, measures, policies, etc.)

Threat identification and scenarios creation

Asset identification and vulnerability analysis

Existing security measures identification

Impact analysis

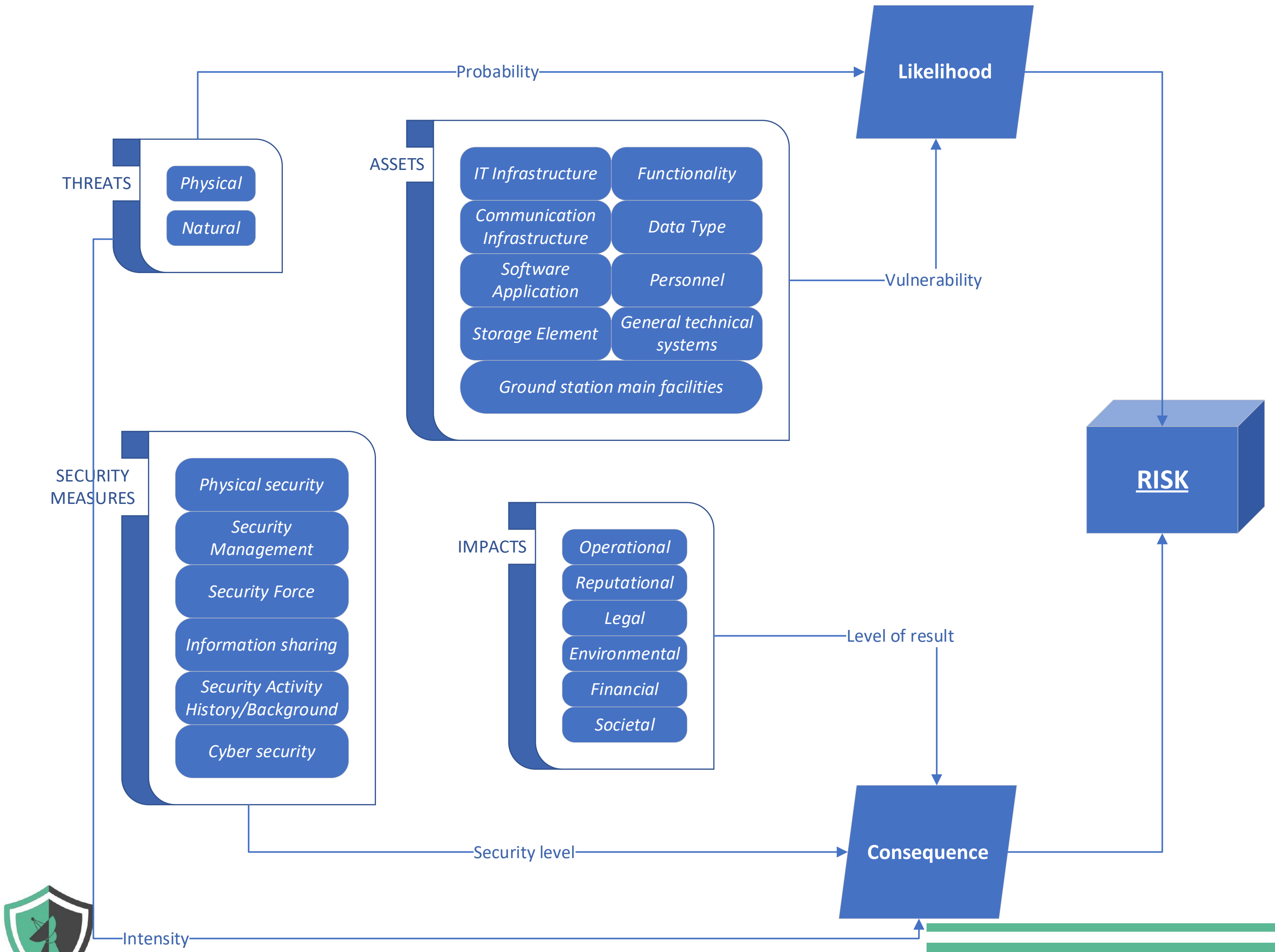
Threat, Vulnerability and Consequence analysis

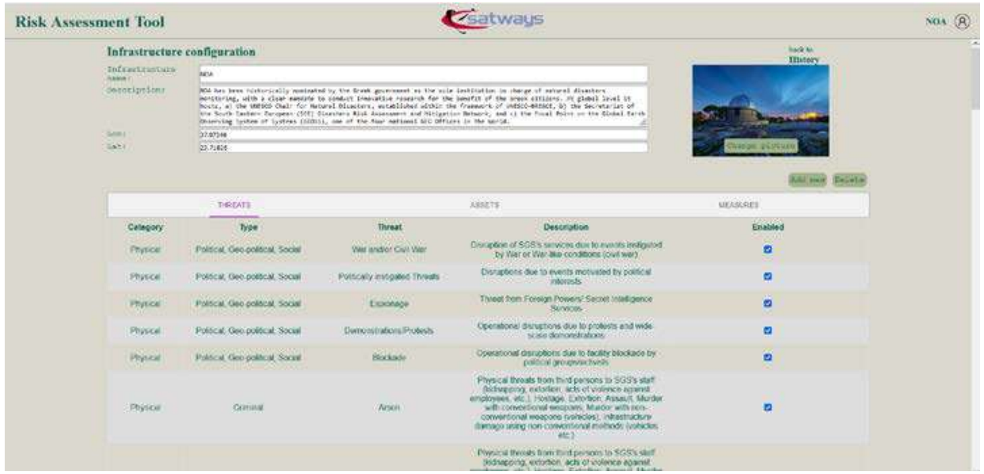
Risk estimation and prioritization

Risk evaluation & mitigation

Recommendation for protection measures & procedures

CIRP-RAT main components





Infrastructure configuration

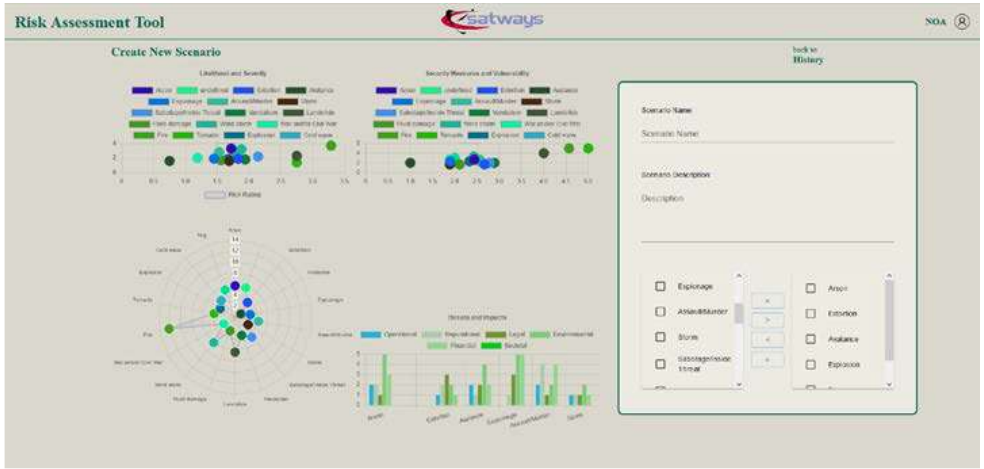
Infrastructure name: NOA

Description: NOA has been historically nominated by the Greek government as the sole institution in charge of natural disasters monitoring, with a clear mandate to conduct innovative research for the benefit of the Greek citizens. At global level it hosts, a) the UNESCO Chair for Natural Disasters, established within the framework of UNESCO-BRESCE, b) the Secretariat of the South Eastern European (SEE) Disasters Risk Assessment and Mitigation Network, and c) the Focal Point on the Global Earth Observing System of Systems (GEOSS), one of the four national GEO Offices in the world.

Lon: 37.97346

Lat: 23.71826

Category	Type	Threat	Description	Enabled
Physical	Political, Geo-political, Social	War and/or Civil War	Disruption of SGS's services due to events instigated by War or War-like conditions (civil war)	☑
Physical	Political, Geo-political, Social	Politically instigated Threats	Disruptions due to events motivated by political interests	☑
Physical	Political, Geo-political, Social	Espionage	Threat from Foreign Powers/ Secret Intelligence Services	☑
Physical	Political, Geo-political, Social	Demonstrations/Protests	Operational disruptions due to protests and wide scale demonstrations	☑
Physical	Political, Geo-political, Social	Blockade	Operational disruptions due to facility blockade by political groups/activists	☑
Physical	Criminal	Arson	Physical threats from third persons to SGS's staff (kidnapping, extortion, acts of violence against employees, etc.), Hostage, Extortion, Assault, Murder with conventional weapons, Murder with non-conventional weapons (vehicles), infrastructure damage using non-conventional methods (vehicles, etc.)	☑
			Physical threats from third persons to SGS's staff (kidnapping, extortion, acts of violence against	



Create New Scenario

Scenario Name

Scenario Name

Scenario Description

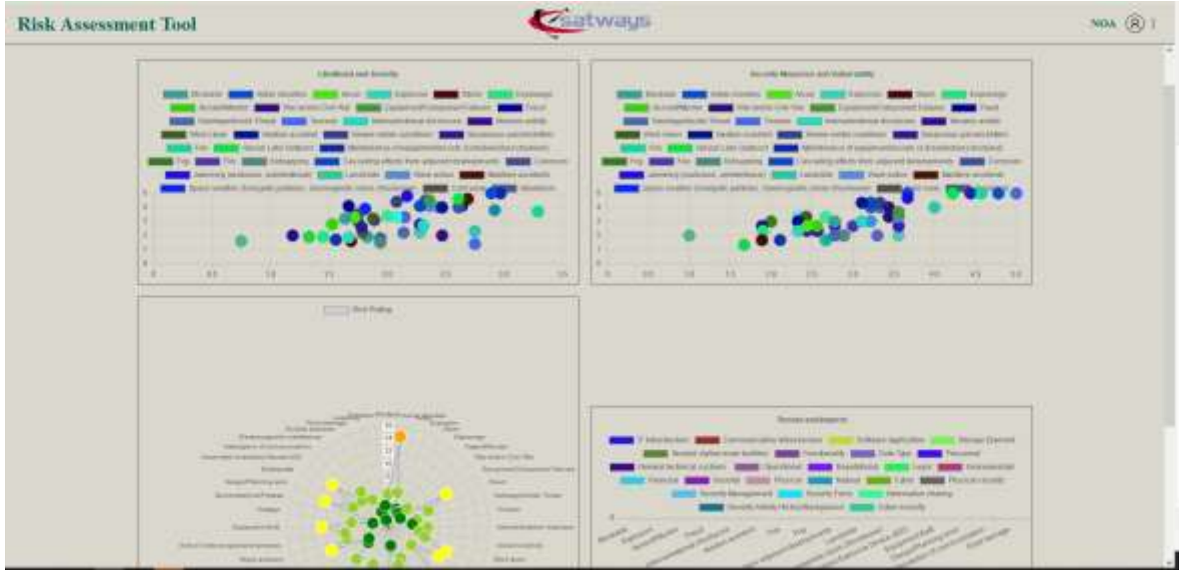
Description

□ Espionage
□ Assault/Murder
□ Storm
□ Sabotage/Insider threat

□ Arson
□ Extortion
□ Avalanche
□ Explosion

CPS4CIP 2022, 20 Sept 2022

CIRP-RAT results for physical threats assessment



Risk Level	Risk Definition
Maximum	Unacceptable: Maximum disruption of provided services and maximum threat to facility operation. Implement new/additional security measures, create/update plans or processes
High	Unacceptable: Maximum disruption of provided services, large threat to facility operation. Implement new/additional security measures, create/update plans or processes
Medium	(Un)acceptable: Some disruption to the provided services, some threat to facility performance. It should be aggressively managed, and consider enhancement of or additional measures.
Low	Acceptable: little disruption, little threat to the facility. Some security actions/measures are probably necessary.
Minimum	Acceptable: No or very small disruption to the facility. The current security framework is sufficient.

Several diagrams and tables are produced, presenting the following information (non-exhaustive):

- Likelihood vs Severity
- Security Measures vs Vulnerability
- Risk Rating
- Threats vs Impacts
- Risk, Severity, Likelihood

Why risk assessment framework and CIRP-RAT?

Risk awareness and informed decision making on security measures

Organized and holistic security plan

Improved allocation of resources

Preparedness and anticipation of threats

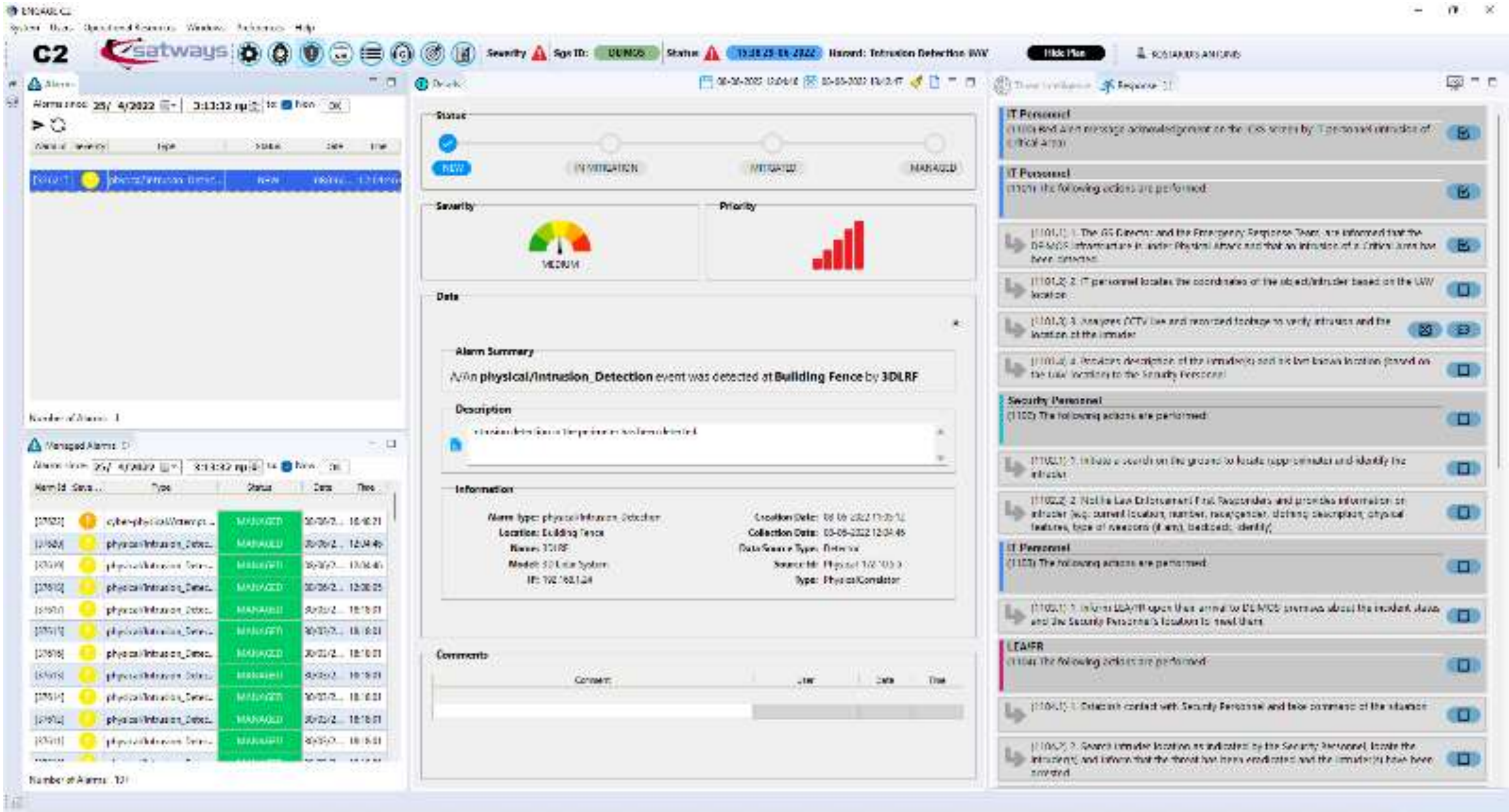
Incident response capacity and mitigation of incident damage

7SHIELD

ENGAGE PSIM

- ✓ Unified User Interface
- ✓ 2D / 3D Map
- ✓ Advanced User & Role management (access rights per user and roles)
- ✓ Collaboration with the FRs on the field (tracking, monitoring, mission assignment)
- ✓ Depiction of situation on the field
- ✓ Integrated Emergency Response Plans

Advanced Graphical User Interface (Thick Client or Web)



Status: NEW

Severity: MEDIUM

Priority

Data

Alarm Summary

A/An **physical/Intrusion_Detection** event was detected at **Building Fence** by **3DLRF**

Description

Information

Alarm type: physical/Intrusion_Detection
Location: Building Fence
Name: 3DLRF
Model: 3D Lidar System
IP: 192.168.1.24

Creation Date: 03-08-2022 12:35:12
Collection Date: 03-08-2022 12:04:46
Data Source Type: Detector
Source Id: Physical 1/2 103.3
Type: Physical/Correlator

IT Personnel
(1100) Red Alert message acknowledgement on the CCS screen by IT personnel (Intrusion of Critical Area)

IT Personnel
(1101) The following actions are performed:

(1101.1) 1. The GS Director and the Emergency Response Team are informed that the DEIMOS infrastructure is under Physical Attack and that an intrusion of a Critical Area has been detected

(1101.2) 2. IT personnel locates the coordinates of the object/intruder based on the UAV location

(1101.3) 3. Analyses CCTV live and recorded footage to verify intrusion and the location of the intruder

(1101.4) 4. Provides description of the intruder(s) and its last known location (based on the UAV location) to the Security Personnel

Security Personnel
(1102) The following actions are performed:

(1102.1) 1. Initiate a search on the ground to locate (approximate) and identify the intruder

(1102.2) 2. Notify Law Enforcement First Responders and provide information on intruder (e.g. current location, number, race/gender, clothing description, physical features, type of weapons (if any), backpack, identity)

IT Personnel
(1103) The following actions are performed:

(1103.1) 1. Inform LEA/FR upon their arrival to DEIMOS premises about the incident status and the Security Personnel's location to meet them

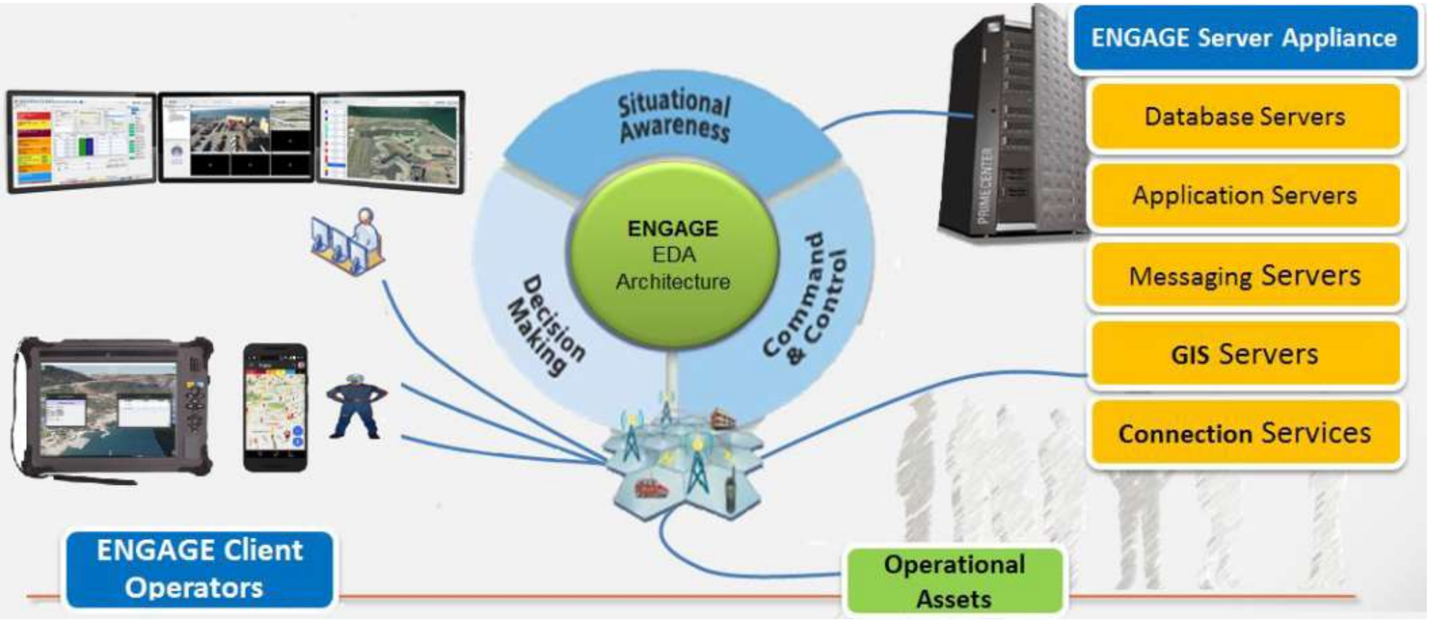
LEA/FR
(1104) The following actions are performed:

(1104.1) 1. Establish contact with Security Personnel and take command of the situation

(1104.2) 2. Search intruder location as indicated by the Security Personnel, locate the intruder(s) and inform that the threat has been eradicated and the intruder(s) have been arrested

7SHIELD

ENGAGE PSIM



- Information from physical and detection tools, event correlators, crisis assessment tools and social media analysis tools are collected and combined. Then they are depicted in the **user-friendly UI, improving the situational awareness** of the users and enabling **effective management of the response activities**.
- Taking into consideration the list of attacks that have been detected and the status of the response activities, an **overall estimation of the CI status is depicted to the users**, informing them about the status of the CI, the overall **severity of the attacks**, the **hazard types** etc.
- During a crisis, the ENGAGE PSIM enables the **communication between the commanders and the FRs**, by providing to the users the **status of the FRs** (e.g. their position and vital signs), and by **collaborating with them and assigning to them commands/missions.**
- During the response phase, the ENGAGE PSIM supports the decision-making process by incorporating the **Emergency Response Plan** of the CIs. These plans **guide the actions of the commanders**, by mentioning which action should be executed in each phase of the crisis (mission assignments, communication of the situation to external agencies, internal actions etc.).
- The person in charge can **manage all resources** (human and non-human) through **multiple communication methods and a holistic visualization.**

Emergency Response Plan (ERP) module

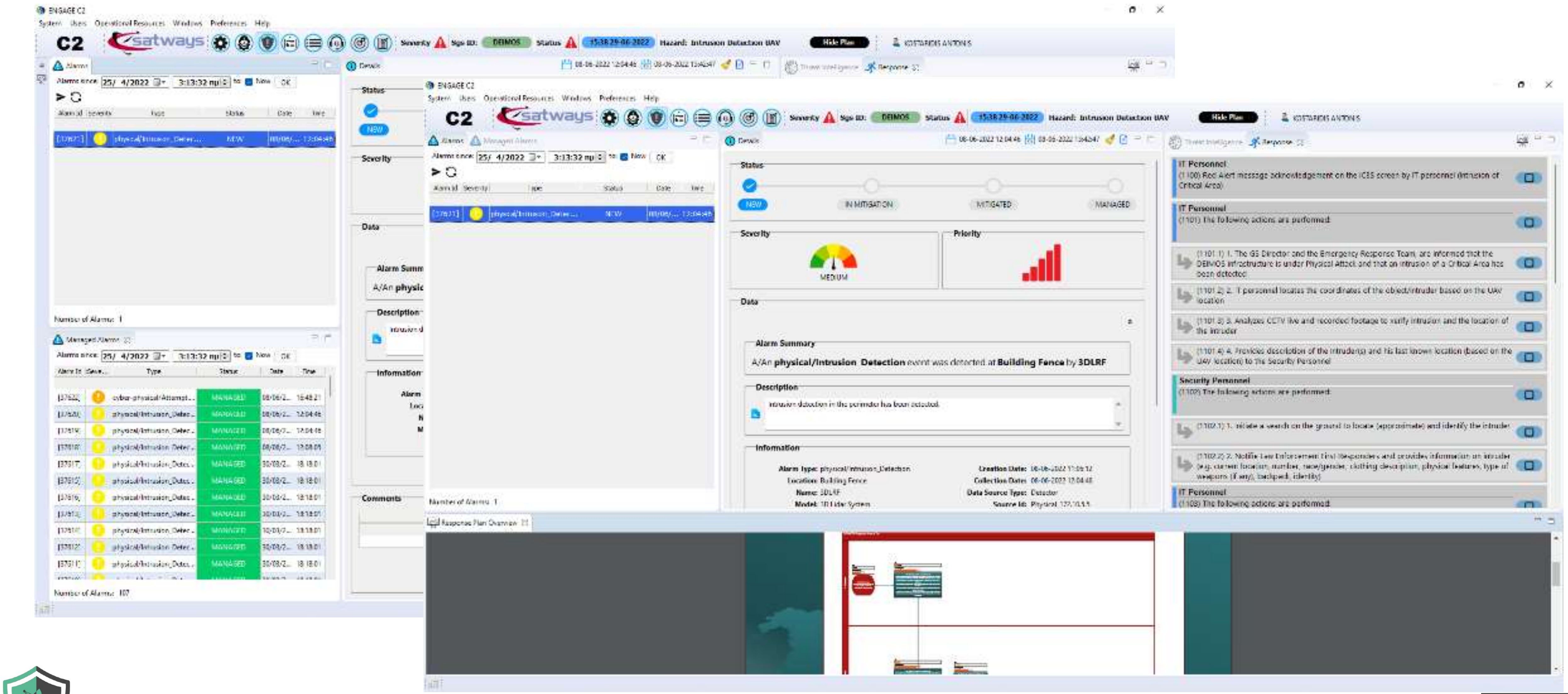
A key part of preparing for an emergency is developing an Emergency Response Plan (ERP). ERPs are set to associate the specific threat events detected or correlated with specific reaction protocols.

- **Improve Operations** by making the right decision in a critical situation [*Elimination of operators panic or subjectivity during response*]
- **Efficient** *[time, cost, quality etc.]* **management** of emergency situations
- **Systematize specific responses** [*Simple, immediate and clear instructions for response actions*]

Emergency Response Plan (ERP) module

Part of ERPs	Components of the ERPs
Strategic: The strategic part of the plans describes the general emergency management policy objectives and offer general guidance by establishing the long-term policy priorities and responsibilities.	1. **Introduction**, **scope** and **purpose** of the ERP 2. The **concept of operations** of the SGS 3. The **operational organization** of the SGS & **assignment of responsibilities** related to emergency management activities 4. **Direction control** and **coordination** identifying the members of the Emergency Response Team and the persons/roles that have operational control over response assets 5. Emergency **information collection**, **analysis,** and **dissemination** 6. **Communications** & **coordination** procedures during the ER 7. **Administration**, **logistics** and **general support policies and services** for all types of emergencies 8. ERP **revision**, **maintenance,** and **training** process
Operational: This part is a detailed organizational process which defines and describes the roles and responsibilities, the tasks, and actions to be performed by the various emergency management stakeholders during response.	9. **Threat/Emergency specific** functional **playbooks** which focus on critical operational functions and who is responsible for carrying them out, or they contain unique and regulatory response details that apply to a specific threat, in the form of standard operating procedures. These playbooks describe policies, processes, roles, and responsibilities that SGS's persons/roles and departments carry out during any pre-identified emergency and until it is resolved.

Emergency Response Plan (ERP) module



Alarms since: 25/ 4/2022 3:13:32 mµ to ☑ Now OK

Alarm Id	Severity	Type	Status	Date	Time
[37621]	●	physical/Intrusion_Deter...	NEW	08/06/...	12:04:46

Number of Alarms: 1

Managed Alarms

Alarms since: 25/ 4/2022 3:13:32 mµ to ☑ Now OK

Alarm Id	Seve...	Type	Status	Date	Time
[37622]	●	cyber-physical/Attempt...	MANAGED	08/06/2...	15:48:21
[37620]	●	physical/Intrusion_Detec...	MANAGED	08/06/2...	12:04:46
[37619]	●	physical/Intrusion_Detec...	MANAGED	08/06/2...	12:04:46
[37618]	●	physical/Intrusion_Detec...	MANAGED	08/06/2...	12:08:05
[37617]	●	physical/Intrusion_Detec...	MANAGED	30/08/2...	18:18:01
[37615]	●	physical/Intrusion_Detec...	MANAGED	30/08/2...	18:18:01
[37616]	●	physical/Intrusion_Detec...	MANAGED	30/08/2...	18:18:01
[37613]	●	physical/Intrusion_Detec...	MANAGED	30/08/2...	18:18:01
[37614]	●	physical/Intrusion_Detec...	MANAGED	30/08/2...	18:18:01
[37612]	●	physical/Intrusion_Detec...	MANAGED	30/08/2...	18:18:01
[37611]	●	physical/Intrusion_Detec...	MANAGED	30/08/2...	18:18:01

Number of Alarms: 107

Details 08-06-2022 12:04:46 08-06-2022 15:42:47

Status: ● NEW ○ IN MITIGATION ○ MITIGATED ○ MANAGED

Severity: MEDIUM

Priority

Data

Alarm Summary

A/An **physical/Intrusion Detection** event was detected at **Building Fence** by **3DLRF**

Description

Intrusion detection in the perimeter has been detected.

Information

Alarm Type: physical/Intrusion_Detection
Location: Building Fence
Name: 3DLRF
Model: 3D Lidar System
Creation Date: 08-06-2022 11:06:12
Collection Date: 08-06-2022 12:04:48
Data Source Type: Detector
Source Id: Physical 172.10.3.5

Comments

Response

IT Personnel
(1100) Red Alert message acknowledgement on the ICSS screen by IT personnel (Intrusion of Critical Area)

IT Personnel
(1101) The following actions are performed

(1101.1) 1. The GS Director and the Emergency Response Team, are informed that the DEIMOS infrastructure is under Physical Attack and that an intrusion of a Critical Area has been detected

(1101.2) 2. IT personnel locates the coordinates of the object/intruder based on the UAV location

(1101.3) 3. Analyzes CCTV live and recorded footage to verify intrusion and the location of the intruder

(1101.4) 4. Provides description of the intruder(s) and his last known location (based on the UAV location) to the Security Personnel

Security Personnel
(1102) The following actions are performed

(1102.1) 1. Initiate a search on the ground to locate (approximate) and identify the intruder

(1102.2) 2. Notifies Law Enforcement First Responders and provides information on intruder (e.g. current location, number, race/gender, clothing description, physical features, type of weapons (if any), backpack, identity)

IT Personnel
(1103) The following actions are performed

7SHIELD

Ilias Gkotsis
i.gkotsis@satways.net
SATWAYS Ltd
https://www.satways.net

7SHIELD

Thank You

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement No 883284.