7SHIELD

INFODAY

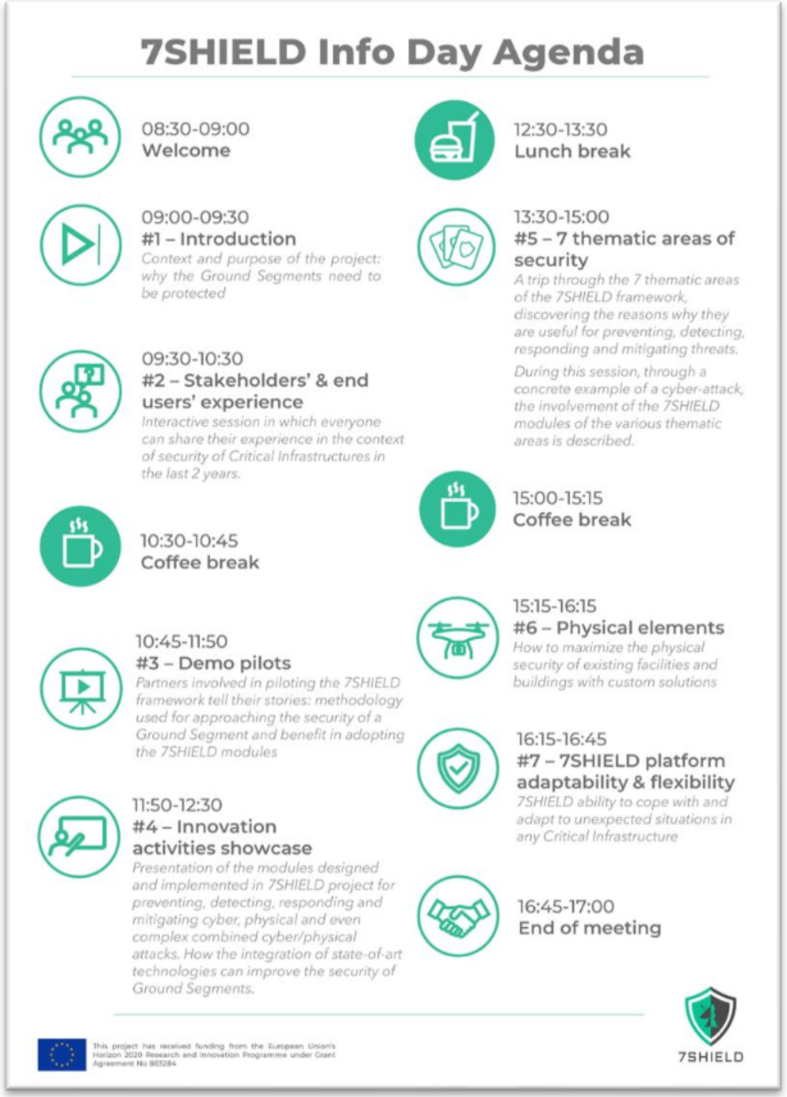
14 December 2022

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

Organized by serco

Objectives

Share how the 7SHIELD framework can protect the Satellite Ground Segments and inform about its flexibility and adaptability in different situation and contexts



7SHIELD Info Day Agenda

08:30-09:00
Welcome

09:00-09:30
#1 – Introduction
Context and purpose of the project: why the Ground Segments need to be protected

09:30-10:30
#2 – Stakeholders' & end users' experience
Interactive session in which everyone can share their experience in the context of security of Critical Infrastructures in the last 2 years.

10:30-10:45
Coffee break

10:45-11:50
#3 – Demo pilots
Partners involved in piloting the 7SHIELD framework tell their stories: methodology used for approaching the security of a Ground Segment and benefit in adopting the 7SHIELD modules

11:50-12:30
#4 – Innovation activities showcase
Presentation of the modules designed and implemented in 7SHIELD project for preventing, detecting, responding and mitigating cyber, physical and even complex combined cyber/physical attacks. How the integration of state-of-art technologies can improve the security of Ground Segments.

12:30-13:30
Lunch break

13:30-15:00
#5 – 7 thematic areas of security
A trip through the 7 thematic areas of the 7SHIELD framework, discovering the reasons why they are useful for preventing, detecting, responding and mitigating threats.

During this session, through a concrete example of a cyber-attack, the involvement of the 7SHIELD modules of the various thematic areas is described.

15:00-15:15
Coffee break

15:15-16:15
#6 – Physical elements
How to maximize the physical security of existing facilities and buildings with custom solutions

16:15-16:45
#7 – 7SHIELD platform adaptability & flexibility
7SHIELD ability to cope with and adapt to unexpected situations in any Critical Infrastructure

16:45-17:00
End of meeting

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 883284

7SHIELD

https://www.7shield.eu/7shield-info-day/

Outcomes

Knowledge of the key results of the 7SHIELD project

Information about the 7SHIELD applicability in the context of the security of Space Ground Segments

Hybrid conference – Instructions

Remote Participation

- There are several interactive sessions but, in case of questions, please use the “hand” button on the Microsoft Teams to raise your hand and talk when we will ask you to do it or use the chat for writing your answer

Physical Participation

- There are several interactive sessions but, in case of questions, please raise your hand and talk when you get a microphone
- Write a post-it and put it on the flipchart on the bottom of the room

Note: the meeting will be registered, pictures will be taken and will be used for LinkedIn posts

Live questionnaires

Use your smartphone to access to a set of questions

- Scan the QR code
- Go to the indicated website and include the code provided
- (no need to download any app or register to any site)

Wi-fi connection provided by the hotel

7SHIELD

#1 - Introduction

Context and purpose of the project: why the Ground Segments needs to be protected

Gabriele Giunta (ENGINEERING ING. INF. SPA)

Project Coordinator

7SHIELD Identity Card

- **WHO**: **22 partners** – including **5 Ground Segment operators**
- **WHAT**: **EC H2020 Grant** under the call **SU-INFRA-2019**
- **WHEN**: 1 September 2020 → 28 February 2023 (**30 months**)
- **WHY**: In response to topic: **SU-INFRA01-2018-2019-2020** “Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe”
- **Mission**: to provide a flexible and holistic **security framework** covering all the **macro-stages of crisis management** (***prevention***, ***detection***, ***response*** and ***mitigation***) to protect **EU Space Ground Segment Infrastructure** against cyber, physical and C/P threats.
- **HOW**: H2020 Innovation Action

7SHIELD

7SHIELD - Consortium

22 Partners
12 European countries

NORWAY
SWEDEN
GERMANY
FRANCE
SPAIN
UKRAINE
ROMANIA

FINNISH METEOROLOGICAL INSTITUTE · spaceapplications SERVICES · deimos elecnor group · serco · IAASARS

5 GSSS infrastructure owners and operators

KEMEA · HELLENIC POLICE · EETT HELLENIC TELECOMMUNICATIONS & POST COMMISSION

3 first responder and policy organizations

CENTRIC Centre of Excellence in Terrorism, Resilience, Intelligence and Organised Crime Research · CERTH CENTRE FOR RESEARCH & TECHNOLOGY HELLAS · CeRICT

3 academic/research institutes

ENGINEERING · CS GROUP · cyberlens · Resilier Business Continuity · deimos elecnor group · satways · CS NOVIDY'S · RESILTECH · r. Frucht Systems Ltd. · inov inesc inovação · ACCELIGENCE

11 large enterprises and technical SMEs

7SHIELD

7SHIELD - Landscape and Baseline (1/3)

SATCOM play a **vital role in the global telecom systems.** We live in a world where an ever-increasing stream of digital data is flowing between continents.

Copernicus Services (Atmosphere, Marine, Land, Climate Change, Security and Emergency), **Defence & Security Apps** (Satcen, Frontex, EMSA), **Low Earth Orbit systems** (International Space Station)

An increasing demand for satellite-based communication and data from space based systems delivering services for today's economy and governments

An increasing number of ground segment infrastructures receive/distribute massive amounts of (satellite) data

7SHIELD - Landscape and Baseline (2/3)

An increasing need for secure spectrum usage. Ground segments increasingly appear as potential “**new targets**” for “**new threats**”, especially the cyber-physical ones

A **cyber/physical attack** would cause cascading impacts on public safety and security of European citizens and affect other European Critical Infrastructure

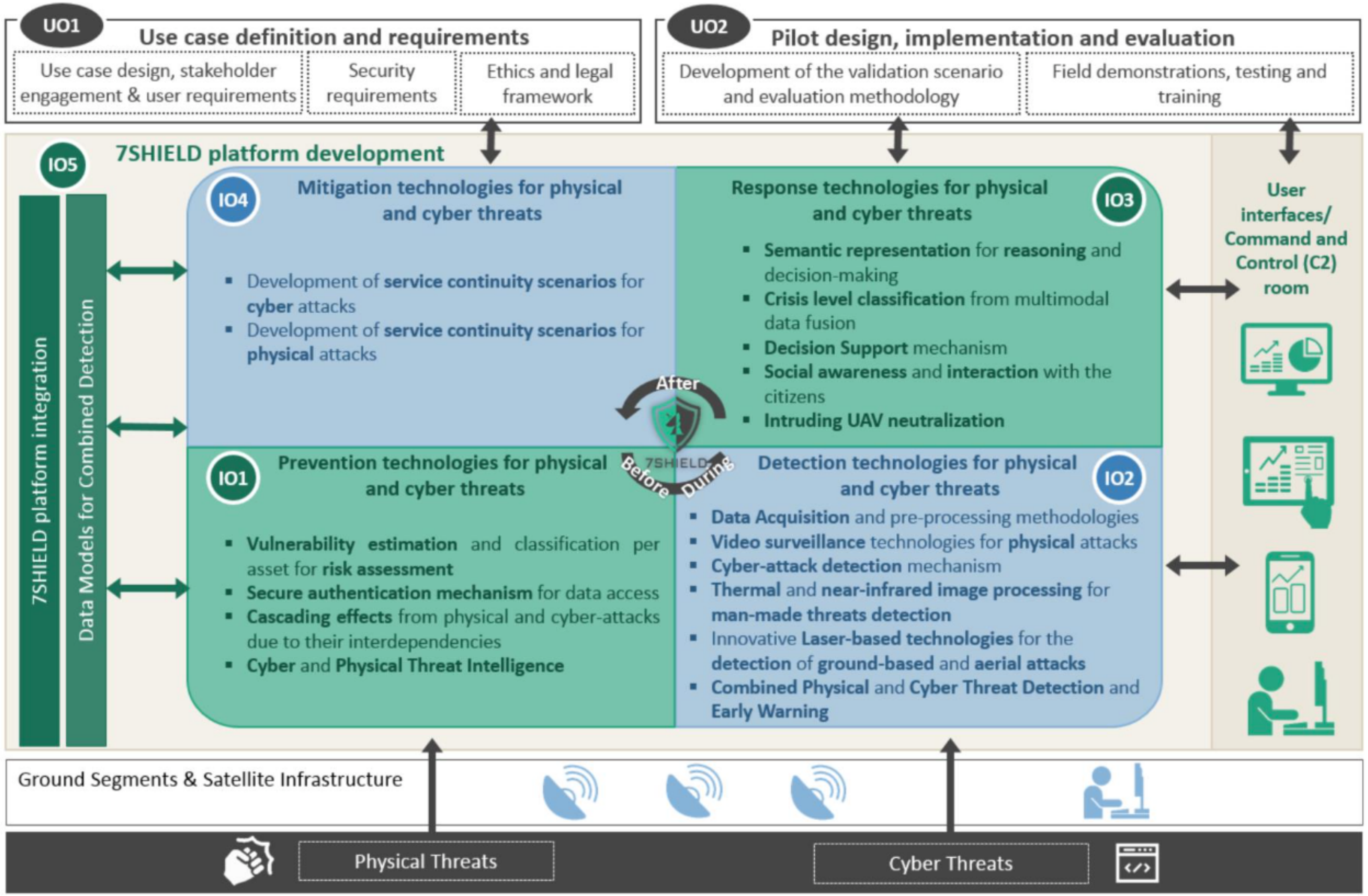
The **physical technologies** are mature, meanwhile, **cybersecurity** depends greatly on physical security. The **cyber-attacks** are increasing in number and in sophistication. The **security budget** of companies is increasing

7SHIELD - Landscape and Baseline (3/2)

- Current approaches are **inadequate** to provide a high-level of protection/resilience of EU Ground Segments
  - Recent advances in surveillance mechanisms with robotic technologies and AI **are not fully exploited or are fragmented**
  - Development of a transparent user-oriented resilience-driven decision support system **is still missing**
  - **Depend heavily** on secure and resilient capabilities
  - **Capabilities rely signifi**cantly on international cooperation to develop norms and standards
  - Standards move slowly and **still considered outdated**

7SHIELD Objectives

- Integrated yet **flexible** and **adaptive** framework
- Deploying **innovative** services
- Integrating advanced **state-of-the-art** technologies
- Contributing to policy making and **standardisation**



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**

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**

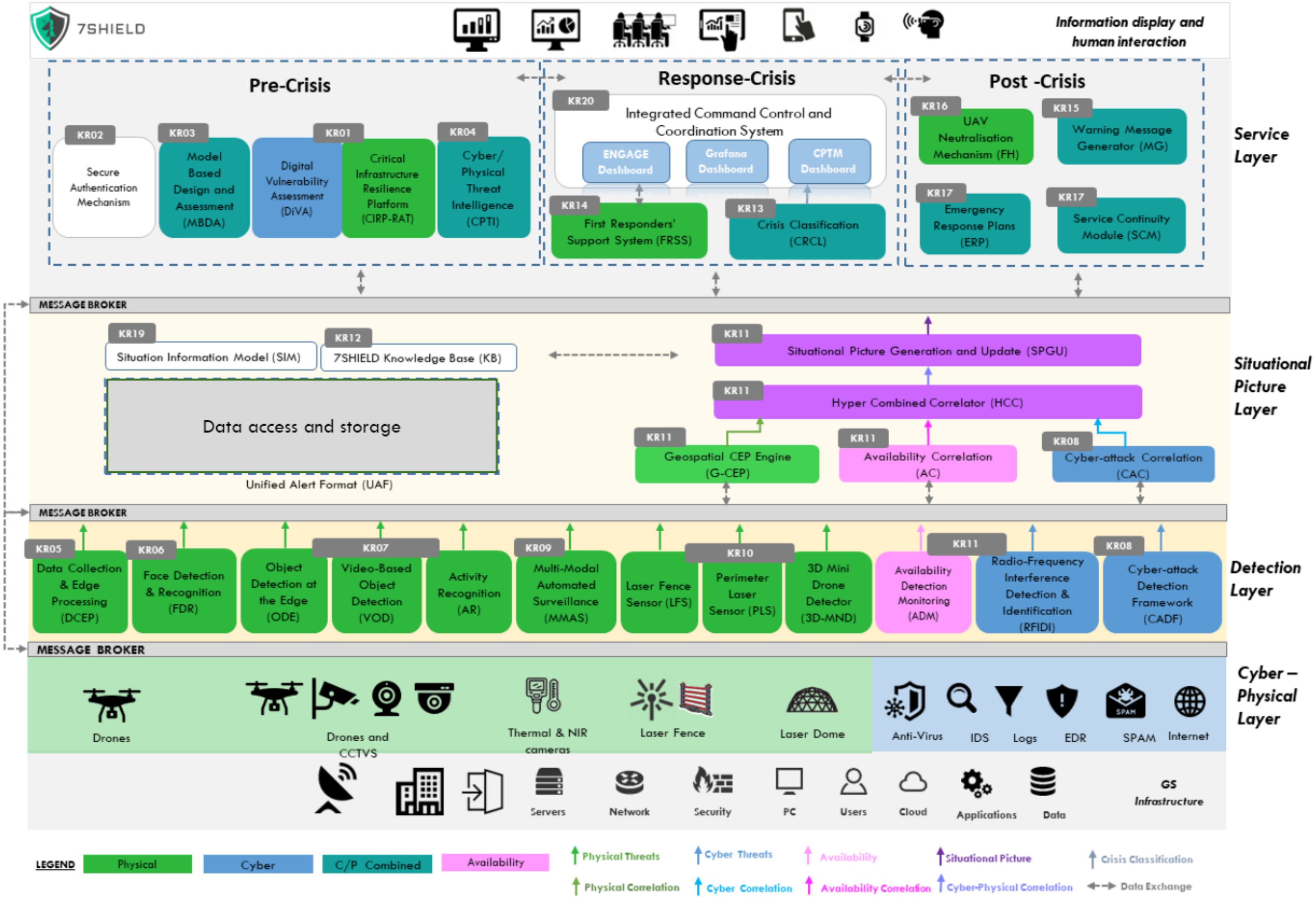
User interfaces/ Command and Control (C2) room

Ground Segments & Satellite Infrastructure

Physical Threats

Cyber Threats

High-Level Architecture of 7SHIELD



7SHIELD

Information display and human interaction

Service Layer

Pre-Crisis

KR02 Secure Authentication Mechanism

KR03 Model Based Design and Assessment (MBDA)

KR01 Digital Vulnerability Assessment (DiVA)

KR01 Critical Infrastructure Resilience Platform (CIRP-RAT)

KR04 Cyber/ Physical Threat Intelligence (CPTI)

Response-Crisis

KR20 Integrated Command Control and Coordination System

ENGAGE Dashboard

Grafana Dashboard

CPTM Dashboard

KR14 First Responders' Support System (FRSS)

KR13 Crisis Classification (CRCL)

Post -Crisis

KR16 UAV Neutralisation Mechanism (FH)

KR15 Warning Message Generator (MG)

KR17 Emergency Response Plans (ERP)

KR17 Service Continuity Module (SCM)

MESSAGE BROKER

Situational Picture Layer

KR19 Situation Information Model (SIM)

KR12 7SHIELD Knowledge Base (KB)

Data access and storage

Unified Alert Format (UAF)

KR11 Situational Picture Generation and Update (SPGU)

KR11 Hyper Combined Correlator (HCC)

KR11 Geospatial CEP Engine (G-CEP)

KR11 Availability Correlation (AC)

KR08 Cyber-attack Correlation (CAC)

MESSAGE BROKER

Detection Layer

KR05 Data Collection & Edge Processing (DCEP)

KR06 Face Detection & Recognition (FDR)

Object Detection at the Edge (ODE)

KR07 Video-Based Object Detection (VOD)

Activity Recognition (AR)

KR09 Multi-Modal Automated Surveillance (MMAS)

Laser Fence Sensor (LFS)

KR10 Perimeter Laser Sensor (PLS)

3D Mini Drone Detector (3D-MND)

Availability Detection Monitoring (ADM)

KR11 Radio-Frequency Interference Detection & Identification (RFIDI)

KR08 Cyber-attack Detection Framework (CADF)

MESSAGE BROKER

Cyber – Physical Layer

Drones

Drones and CCTVS

Thermal & NIR cameras

Laser Fence

Laser Dome

Anti-Virus

IDS

Logs

EDR

SPAM

Internet

Servers

Network

Security

PC

Users

Cloud

Applications

Data

GS Infrastructure

LEGEND

🟩 Physical

🟦 Cyber

🟦 C/P Combined

🟪 Availability

↑ Physical Threats

↑ Physical Correlation

↑ Cyber Threats

↑ Cyber Correlation

↑ Availability

↑ Availability Correlation

↑ Situational Picture

↑ Cyber-Physical Correlation

↑ Crisis Classification

←→ Data Exchange

7SHIELD

7SHIELD Pilots (1/3)

serco ONDA

Cyber-attacks (**Man-In-The-Middle, Ransomware and Distributed Denial of Service**) on the ONDA Copernicus DIAS platform.

✓ **Operational Test executed fully remotely in SEPTEMBER 2021**

spaceapplications SERVICES

Threat detection (**Login brute force attack, Denial of Service and User escalation privileges**) and mitigation on ground segment of the ICE Cubes Service onboard the International Space Station.

✓ **Operational Test executed fully remotely in NOVEMBER 2021**

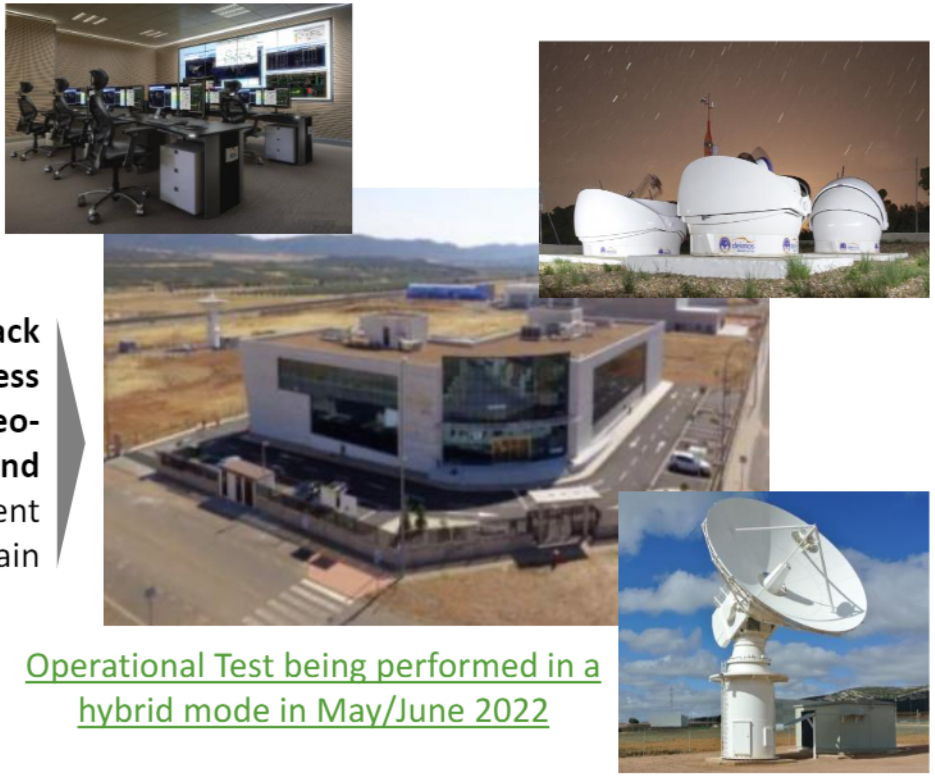
✓ **al DEMO executed in DECEMBER 2022**

7SHIELD Pilots (2/3)

Cyber-physical attack (**Unauthorised access to NOA-IAASARS building and 2 parallel small-scale cyber-attacks**) in the ground segment of NOA, Athens.

✓ Operational Test executed in a hybrid mode in MARCH 2022

✓ al DEMO executed in SEPTEMBER 2022



Cyber-physical attack **(Brute force attack along with an unauthorised access detected by laser-based and video-based tools, UAV intrusion and detection)** in DEIMOS Ground Segment in Spain

✓ Operational Test being performed in a hybrid mode in May/June 2022

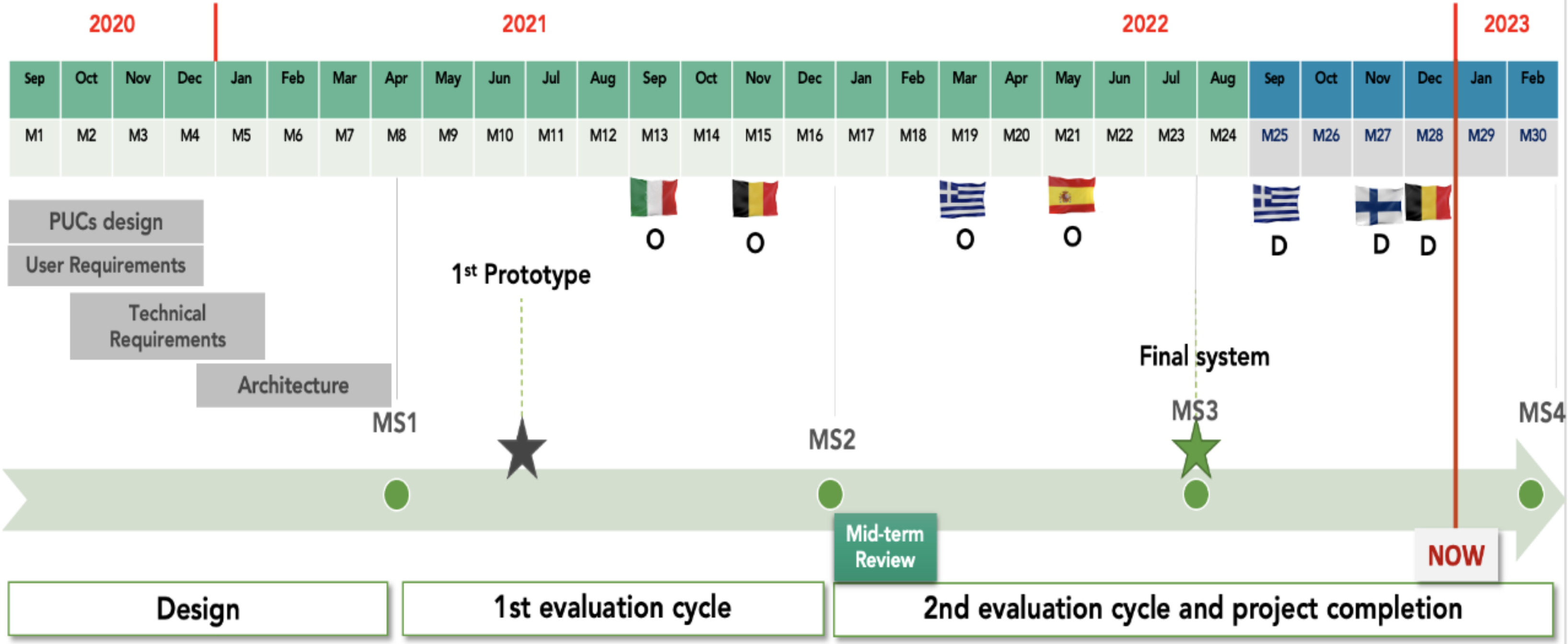
7SHIELD Pilots (3/3)

FINNISH METEOROLOGICAL INSTITUTE

Physical attack in Arctic Space Centre in Sodankylä, Finland will take place in October 2022

✓ al DEMO executed in NOVEMBER 2022

TIME PLAN

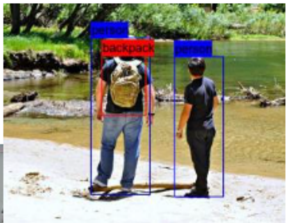


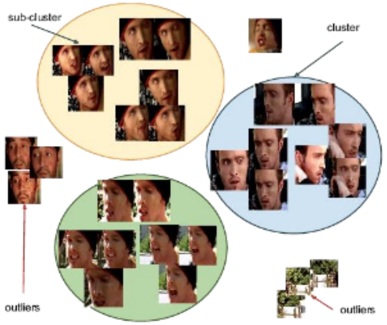
2020				2021												2022												2023	
Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb
M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	M13	M14	M15	M16	M17	M18	M19	M20	M21	M22	M23	M24	M25	M26	M27	M28	M29	M30

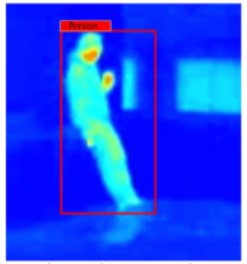
O: Operational test
D: Demo

Detection technologies for cyber and physical threats

- **DETECTORS** to collect “*EVENTS*” captured by sensors deployed in the cyber-physical layer, to inspect and analyse them and to notify as “*ALERT*” only those are mostly noticeable/relevant:
  - PHISICAL 🇪🇸 🇬🇷 🇫🇮
    - Data Collection and Edge Processing (DCEP)
    - Object Detection at the Edge (ODE)
    - Face Detection and Recognition (FDR)
    - Video-based Object Detection (VOD)
    - MultiModal Automated Surveillance System (MMAS)
    - Perimeter Laser Sensor (PLS)
    - Laser Fence Sensor (LFS)
    - 3-Dimensional Mini drone (3D-MND)
  - CYBER 🇮🇹 🇧🇪 🇪🇸 🇬🇷 🇫🇮
    - Network Intrusion Detection System (NIDS)
    - Endpoint Detection and Response System (EDRS)
    - File Integrity (FI)
  - Availability 🇮🇹 🇧🇪 🇪🇸 🇬🇷 🇫🇮
    - Availability Detection Monitoring (ADM)
    - RF Interference Detector (RFID)



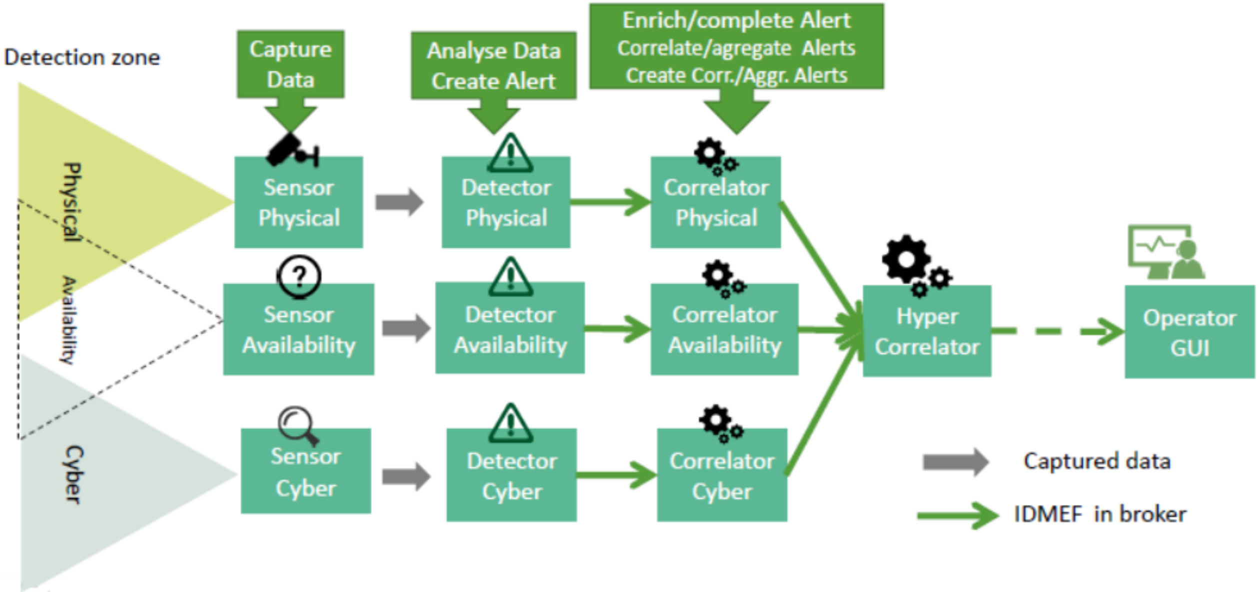




Thermal image with classification alarms

Correlation technologies for cyber and physical threats

- **CORRELATORS** to validate, enrich, aggregate and correlate the notified alerts on cyber or physical threats, creating new alerts on cyber and/or physical incidents/attacks.



- PHYSICAL: Geospatial CEP Engine (G-CEP) 🇪🇸 🇬🇷 🇫🇮
- CYBER: Cyber-Attack Correlator (CAC) 🇮🇹 🇧🇪 🇪🇸 🇬🇷 🇫🇮
- CYBER-PHYSICAL: Hyper-Combined Correlator (HCC) 🇧🇪 🇪🇸 🇬🇷 🇫🇮
- OTHER: Availability Correlator (AC) 🇧🇪 🇪🇸 🇬🇷 🇫🇮

Prevention tools for cyber and physical threats

- **Data Confidentiality and Integrity Service** to provide a robust identity management tool for **multi-factor authentication**, data integrity and confidentiality. 🇮🇹 🇧🇪 🇪🇸 🇬🇷 🇫🇮

- **Model Based Design and Assessment** to **model the overall infrastructure** and its hierarchical decomposition, in terms of **assets to be protected**, their interfaces and the messages exchanged between them, considering the **dependencies** between different components. 🇮🇹 🇧🇪 🇪🇸 🇬🇷 🇫🇮

- **Critical Infrastructure Resilience Platform** and **Digital Vulnerability Assessment Tool** to **model the Critical Infrastructure assets** and to **identify the threat agents** and the **attack strategies** that could compromise them, performing respectively a cyber and physical risk assessment on hazards.
  🇮🇹 🇧🇪 🇪🇸 🇬🇷 🇫🇮

- **Cyber-Physical Threat Intelligent** to **search, monitor and analyse C/P threats** across multiple sources (e.g. Dark Web and Underground communities and marketplaces, social media networks, blogs, forum, etc.).

🇮🇹 🇧🇪 🇪🇸 🇬🇷 🇫🇮

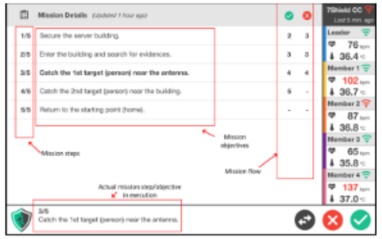
Response tools for cyber and physical threats

- **Crisis Classification Module** to enhance the decision-making processes, by providing **real-time (or “near” real-time) assessments** of the **severity level** of an ongoing physical and/or cyber-attack in critical satellite and ground segments. 🇧🇪 🇪🇸 🇬🇷 🇫🇮

- **Social Awareness and Warning Message** to construct concise and informative messages to disseminate to a variety of stakeholders (e.g. citizens, FRs, SGS employees) about the occurrence of an incident, the immediate consequences and any action should be taken 🇧🇪 🇬🇷 🇫🇮

- **First Responders Support System** to enable **FR teams to be self-aware** and have more information to support effective decision making in the field without an infrastructure or C2 support.

🇬🇷 🇫🇮

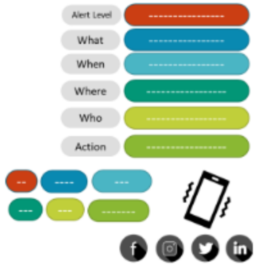


Mission Details (Updated 1 hour ago)

		✓	✗
1/5	Secure the server building.	2	3
2/5	Enter the building and search for evidences.	3	3
3/5	**Catch the 1st target (person) near the antenna.**	4	4
4/5	Catch the 2nd target (person) near the building.	5	-
5/5	Return to the starting point (home).	-	-

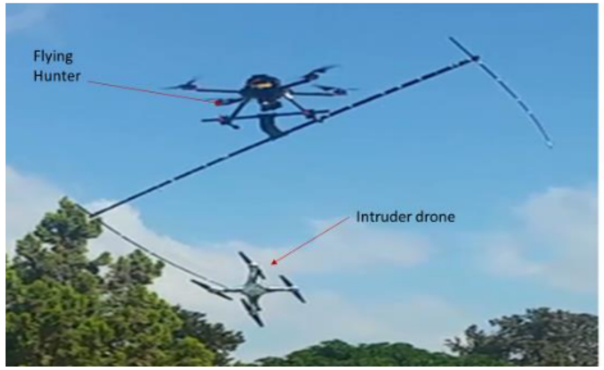
7Shield CC Last 5 min. ago	
Leader	76 bpm 36.4 °C
Member 1	102 bpm 36.7 °C
Member 2	87 bpm 36.8 °C
Member 3	65 bpm 35.8 °C
Member 4	137 bpm 37.0 °C

3/5
Catch the 1st target (person) near the antenna.

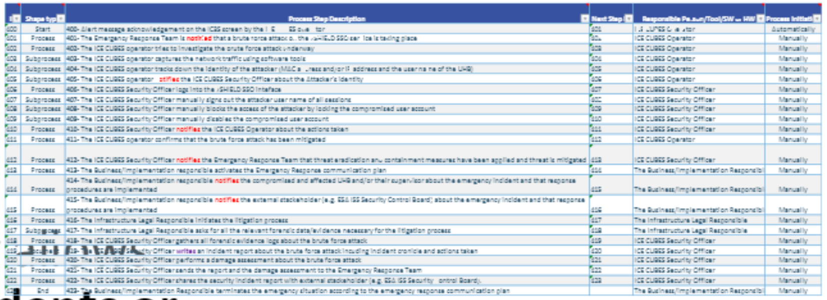


Response tools for cyber and physical threats

- **Flying Hunter** is a specially assembled drone which flies towards the intruding drone and **catches the intruding drone using the net hung** under belly, brings the drone to a predesignated location on the ground, and drops it there.



- **Emergency Response Plans (ERPs)** include **strategies, procedures, best practices** and **systems** commonly required for response and recovery.

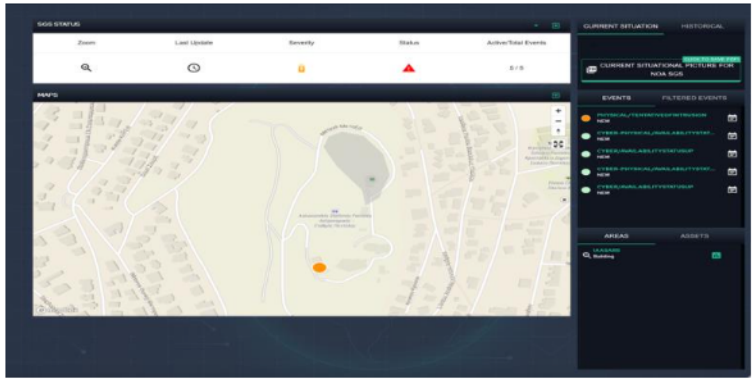


ID	Shape typ	Process Step Description	Next Step I	Responsible Person/Tool/SW or HW	Process Initiati
400	Start	400- Alert message acknowledgement on the ICSS screen by the ICE CUBES Operator	401	ICE CUBES Operator	Automatically
401	Process	401- The Emergency Response Team is notified that a brute force attack on the 7SHIELD SSO service is taking place	402	ICE CUBES Operator	Manually
402	Process	402- The ICE CUBES operator tries to investigate the brute force attack underway	403	ICE CUBES Operator	Manually
403	Subprocess	403- The ICE CUBES operator captures the network traffic using software tools	404	ICE CUBES Operator	Manually
404	Subprocess	404- The ICE CUBES operator tracks down the identity of the attacker (MAC address and/or IP address and the user name of the UHB)	405	ICE CUBES Operator	Manually
405	Subprocess	405- The ICE CUBES operator notifies the ICE CUBES Security Officer about the Attacker's identity	406	ICE CUBES Operator	Manually
406	Process	406- The ICE CUBES Security Officer logs into the 7SHIELD SSO Inteface	407	ICE CUBES Security Officer	Manually
407	Subprocess	407- The ICE CUBES Security Officer manually signs out the attacker user name of all sessions	408	ICE CUBES Security Officer	Manually
408	Subprocess	408- The ICE CUBES Security Officer manually blocks the access of the attacker by locking the compromised user account	409	ICE CUBES Security Officer	Manually
409	Subprocess	409- The ICE CUBES Security Officer manually disables the compromised user account	410	ICE CUBES Security Officer	Manually
410	Process	410- The ICE CUBES Security Officer notifies the ICE CUBES Operator about the actions taken	411	ICE CUBES Security Officer	Manually
411	Process	411- The ICE CUBES operator confirms that the brute force attack has been mitigated	412	ICE CUBES Operator	Manually
412	Process	412- The ICE CUBES Security Officer notifies the Emergency Response Team that threat eradication and containment measures have been applied and threat is mitigated	413	ICE CUBES Security Officer	Manually
413	Process	413- The Business/Implementation responsible activates the Emergency Response communication plan	414	The Business/Implementation Responsibl	Manually
414	Process	414- The Business/Implementation responsible notifies the compromised and affected UHB and/or their supervisor about the emergency incident and that response procedures are implemented	415	The Business/Implementation Responsibl	Manually
415	Process	415- The Business/Implementation responsible notifies the external stackeholder (e.g. ESA ISS Security Control Board) about the emergency incident and that response procedures are implemented	416	The Business/Implementation Responsibl	Manually
416	Process	416- The Infrastructure Legal Responsible initiates the litigation process	417	The Infrastructure Legal Responsible	Manually
417	Subprocess	417- The Infrastructure Legal Responsible asks for all the relevant forensic data/evidence necessary for the litigation process	418	The Infrastructure Legal Responsible	Manually
418	Process	418- The ICE CUBES Security Officer gathers all forensic evidence logs about the brute force attack	419	ICE CUBES Security Officer	Manually
419	Document	419- The ICE CUBES Security Officer writes an incident report about the brute force attack incuding incident cronicle and actions taken	420	ICE CUBES Security Officer	Manually
420	Process	420- The ICE CUBES Security Officer performs a damage assessment about the brute force attack	421	ICE CUBES Security Officer	Manually
421	Process	421- The ICE CUBES Security Officer sends the report and the damage assessment to the Emergency Response Team	422	ICE CUBES Security Officer	Manually
422	Process	422- The ICE CUBES Security Officer shares the security incident report with external stackeholder (e.g. ESA ISS Security Control Board).	423	ICE CUBES Security Officer	Manually
423	End	423- The Business/Implementation Responsible terminates the emergency situation according to the emergency response communication plan		The Business/Implementation Responsibl	Manually

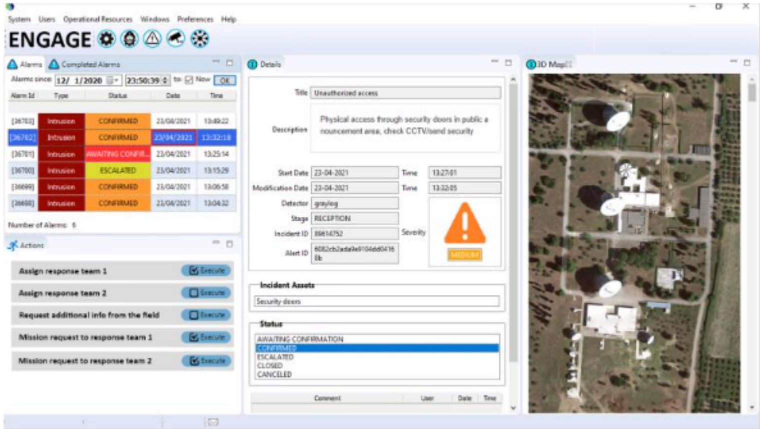
- **Generalized Operational Business Model Tool for Service Continuity** for a **better, faster and more efficient response to emergencies**, **incidents or crises**, with rapid and tested reactions, in order to minimize impact and time to recover.

7SHIELD Command and Control User Interface

- **Cyber Physical Threat Monitoring** provides advance capabilities for **semi-automated monitoring** of the SGS CI **security and intelligent early warning** in case of detected anomalies, C/P attacks or hazards
  - It provides a '**single point of entry**' for users allowing them to access all of the relevant up-to-date information


SGS STATUS
Zoom
Last Update
Severity
Status
Active/Total Events
5 / 5
MAPS
CURRENT SITUATION
HISTORICAL
CLICK TO SAVE PDF
CURRENT SITUATIONAL PICTURE FOR NOA SGS
EVENTS
FILTERED EVENTS
PHYSICAL/TENTATIVEOFINTRUSION
NEW
CYBER-PHYSICAL/AVAILABILITYSTAT...
NEW
CYBER/AVAILABILITYSTATUSUP
NEW
CYBER-PHYSICAL/AVAILABILITYSTAT...
NEW
CYBER/AVAILABILITYSTATUSUP
NEW
AREAS
ASSETS
IAASARS
Building

- **ENGAGE Dashboard and Visual Analytics** supports the **response activities** are related to specific incidents on the Ground Station by **informing users about the situation**, helping them to organise the response activities, **enabling the communication with the FRs** on the field



Alarms since: 12/ 1/2020 23:50:39 to: ☑ Now

Alarm Id	Type	Status	Date	Time
[36703]	Intrusion	CONFIRMED	23/04/2021	13:49:22
[36702]	Intrusion	CONFIRMED	23/04/2021	13:32:18
[36701]	Intrusion	AWAITING CONFIR...	23/04/2021	13:25:14
[36700]	Intrusion	ESCALATED	23/04/2021	13:15:29
[36699]	Intrusion	CONFIRMED	23/04/2021	13:06:58
[36698]	Intrusion	CONFIRMED	23/04/2021	13:04:32

Number of Alarms: 6

Actions

Assign response team 1	☑ Execute
Assign response team 2	□ Execute
Request additional info from the field	□ Execute
Mission request to response team 1	☑ Execute
Mission request to response team 2	☑ Execute

Title: Unauthorized access

Description: Physical access through security doors in public a nouncement area, check CCTV/send security

Start Date: 23-04-2021 Time: 13:27:01

Modification Date: 23-04-2021 Time: 13:32:05

Detector: graylog

Stage: RECEPTION

Incident ID: 89814752

Alert ID: 6082cb2ada9e9104dd0416 8b

Severity: MEDIUM

Incident Assets

Security doors

Status

AWAITING CONFIRMATION
CONFIRMED
ESCALATED
CLOSED
CANCELED

Comment	User	Date	Time

Key achievements in a nutshell

- **ALL component successfully integrated** (26 Modules and 20 Key Results)
- **Validation done in five substantial pilots**:
  - ONDA Copernicus DIAS platform (SERCO, Italy)
  - ICE Cubes Service onboard the ISS (SPACEAPPS, Belgium)
  - DEIMOS Ground Segment (DEIMOS, Spain)
  - NOA Ground Segment (NOA, Greece)
  - Arctic Space Centre (FMI, Finland)
- Covering a diversity and complementarity of **user requirements** enabling true convergence of cyber and physical security
- Covering a variety of **high-impact threat scenarios** to SGS Cis
- Concrete examples of the **threats and attacks** for which 7SHIELD delivers efficient support

Thank You

7SHIELD

Gabriele Giunta: gabriele.giunta@eng.it

7SHIELD website: https://www.7shield.eu/

LinkedIn page: https://www.linkedin.com/company/7shield/

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