



## #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 can the integration of state-of-art technologies improve the security of Ground Segments*





# Pre crisis management

Irene Bicchierai (RESIL)  
WP3 leader





# Prevention technologies for physical and cyber threats

**7SHIELD**

**assesses the  
weaknesses and  
vulnerabilities of each  
asset of the Space  
Ground Segment**





The involved technologies provide

- vulnerabilities estimation and classification for risk assessment
- secure authentication mechanism for data access
- cascade effects from combined cyber-physical attacks
- cyber and physical threat intelligence models





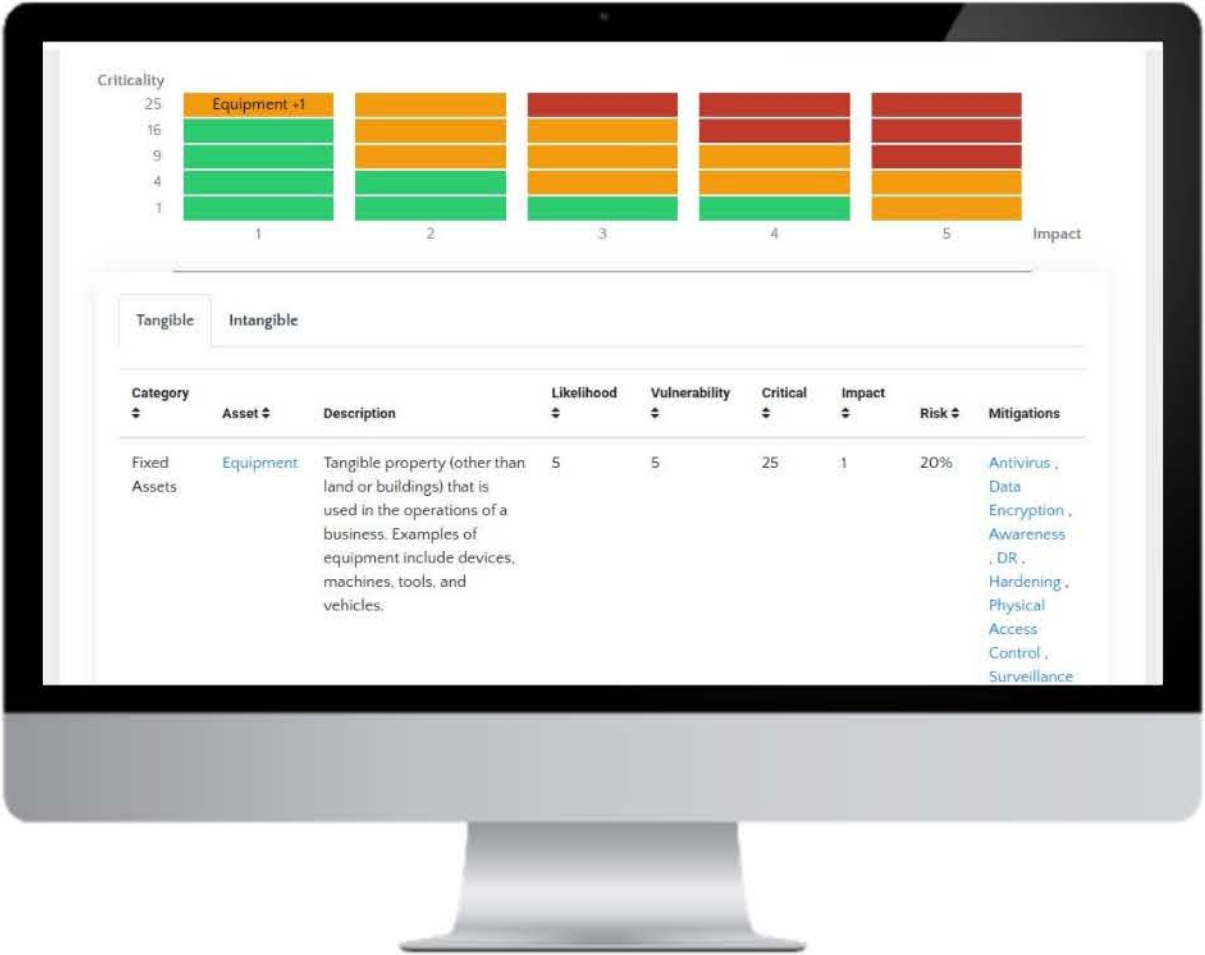
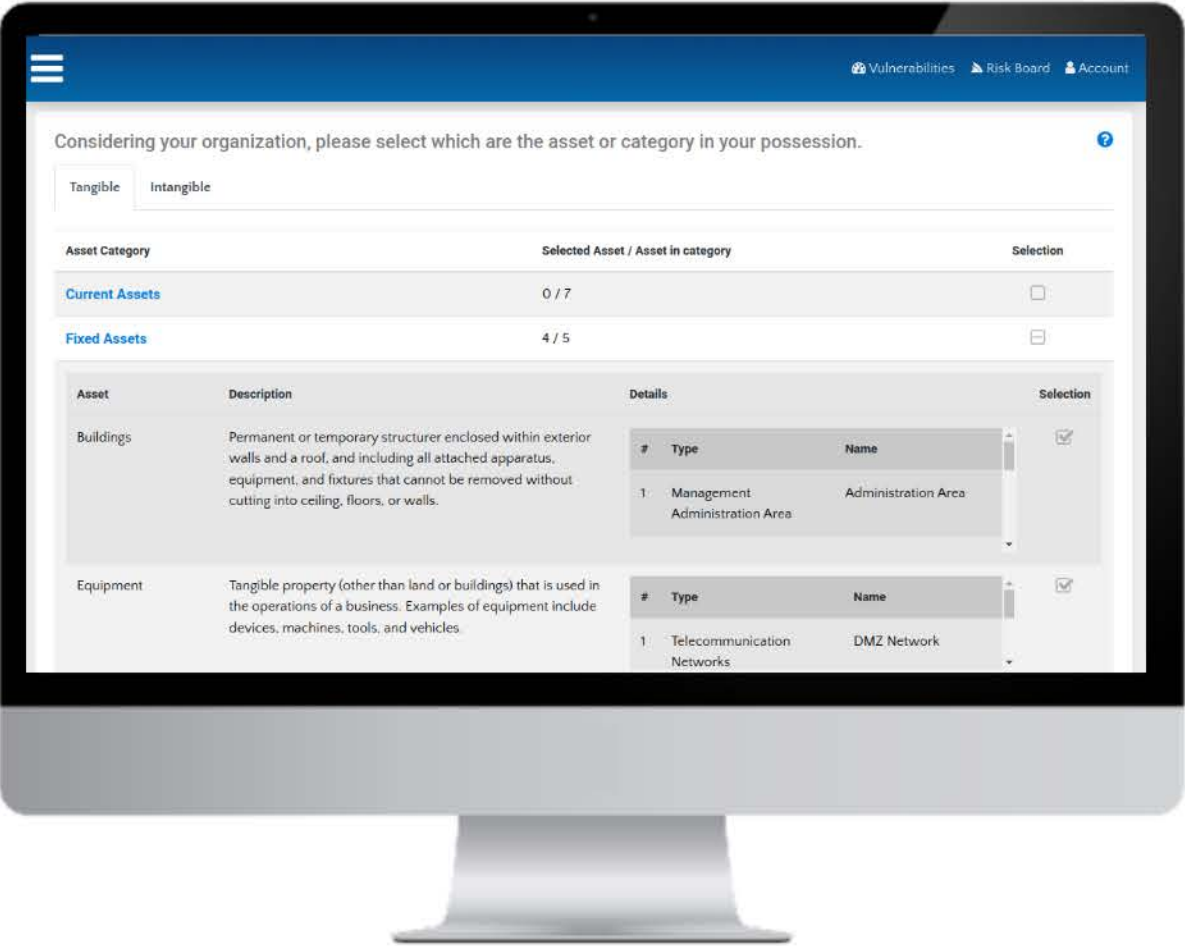
# Vulnerability estimation and classification per asset for risk assessment

Aiming at developing an holistic risk assessment framework to assess cyber and natural/physical threats

By understanding the vulnerability levels of assets of GS Systems, the operators can better plan response and mitigation actions

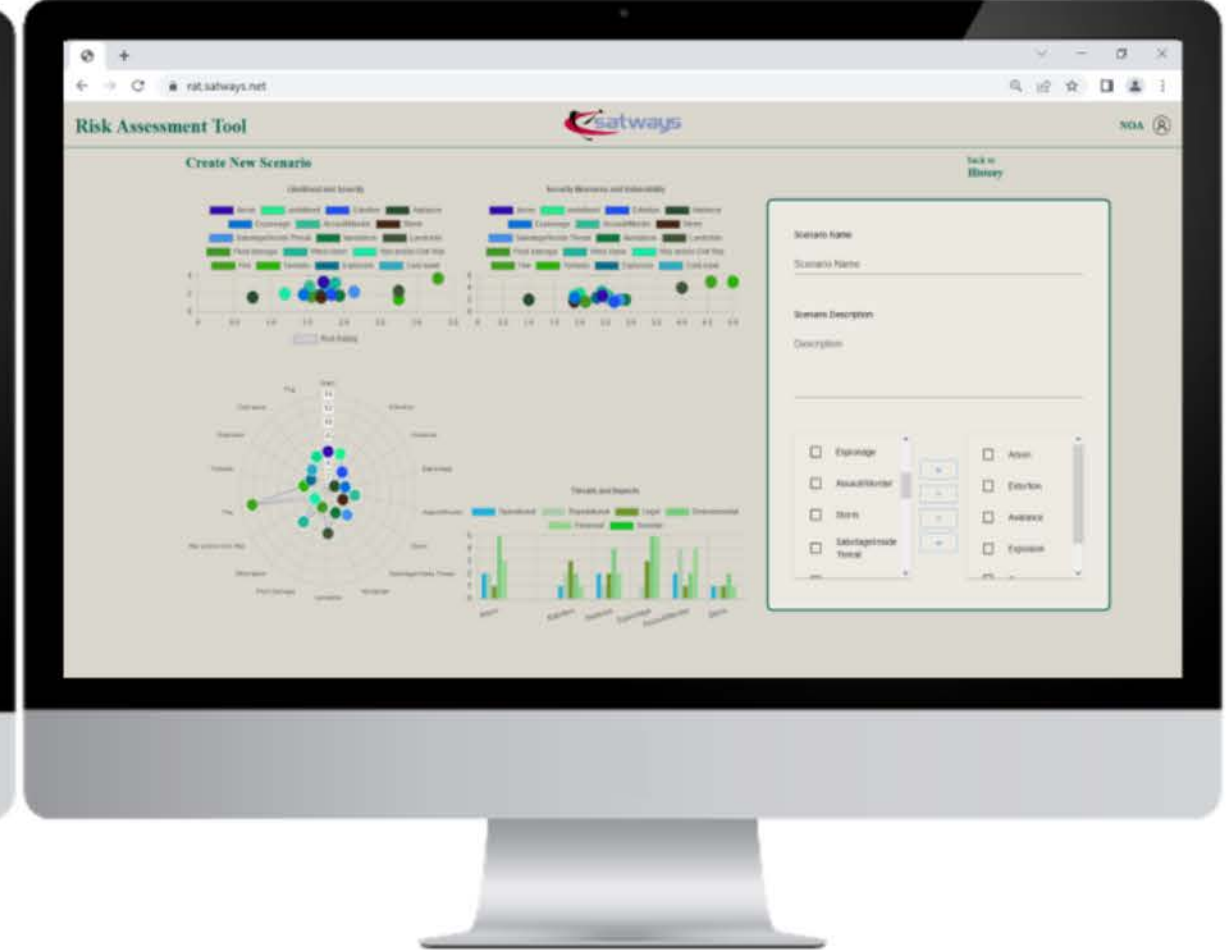
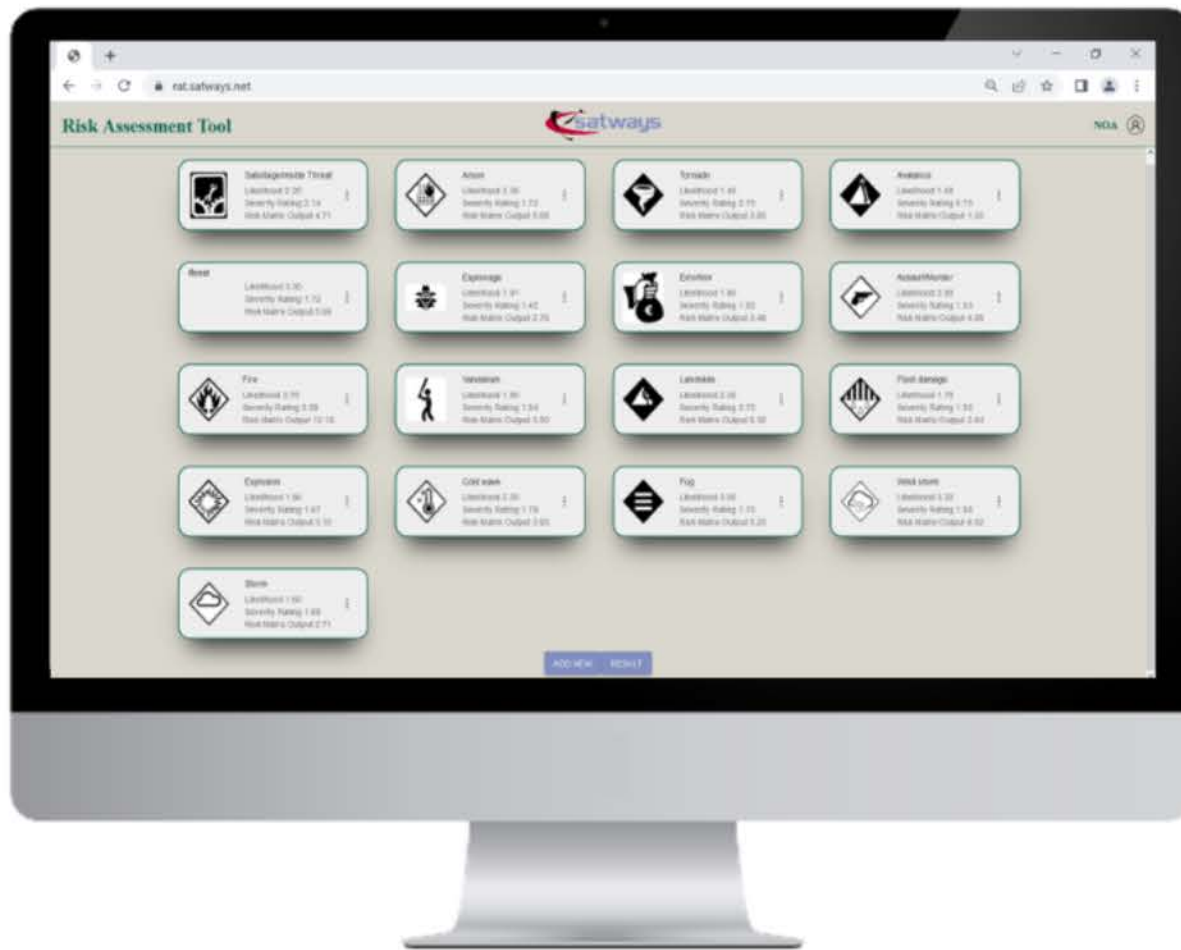


# Cyber Risk Assessment





# Physical and Natural Risk Assessment







# Secure authentication mechanism for data access

The implementation of a secured authentication and authorization mechanism to access the Ground Segment core functions, like the data storages, is critical for the long-term data preservation



- Confidentiality, integrity, availability of data protected from falsification or modification
- Alternative passwordless authentication methods

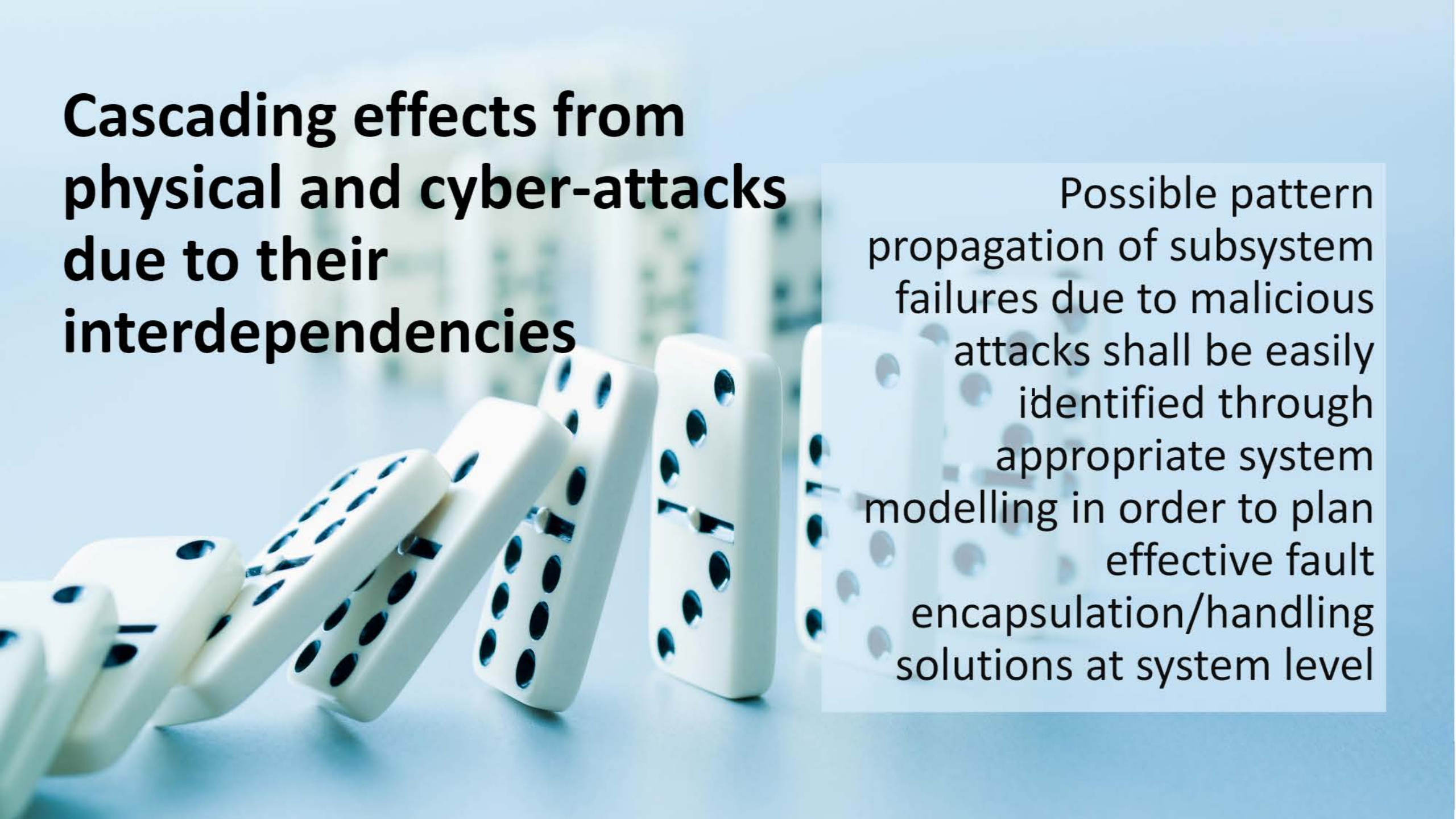




- 
- The background of the slide is a complex, abstract digital pattern. It features concentric circles and rings of varying shades of blue and teal, creating a sense of depth and rotation. Overlaid on these are numerous small, rectangular blocks and lines, some of which are semi-transparent, giving the impression of data being processed or visualized. The overall effect is a high-tech, futuristic aesthetic.
- Kubernetes clusters orchestration
  - Open-source software
  - Hyperledger database
  - Follow FIDO alliance standards



# Cascading effects from physical and cyber-attacks due to their interdependencies

A row of white dominoes is shown falling in a line from left to right. The dominoes are white with black pips. The background is a blurred cityscape with tall buildings under a blue sky.

Possible pattern propagation of subsystem failures due to malicious attacks shall be easily identified through appropriate system modelling in order to plan effective fault encapsulation/handling solutions at system level

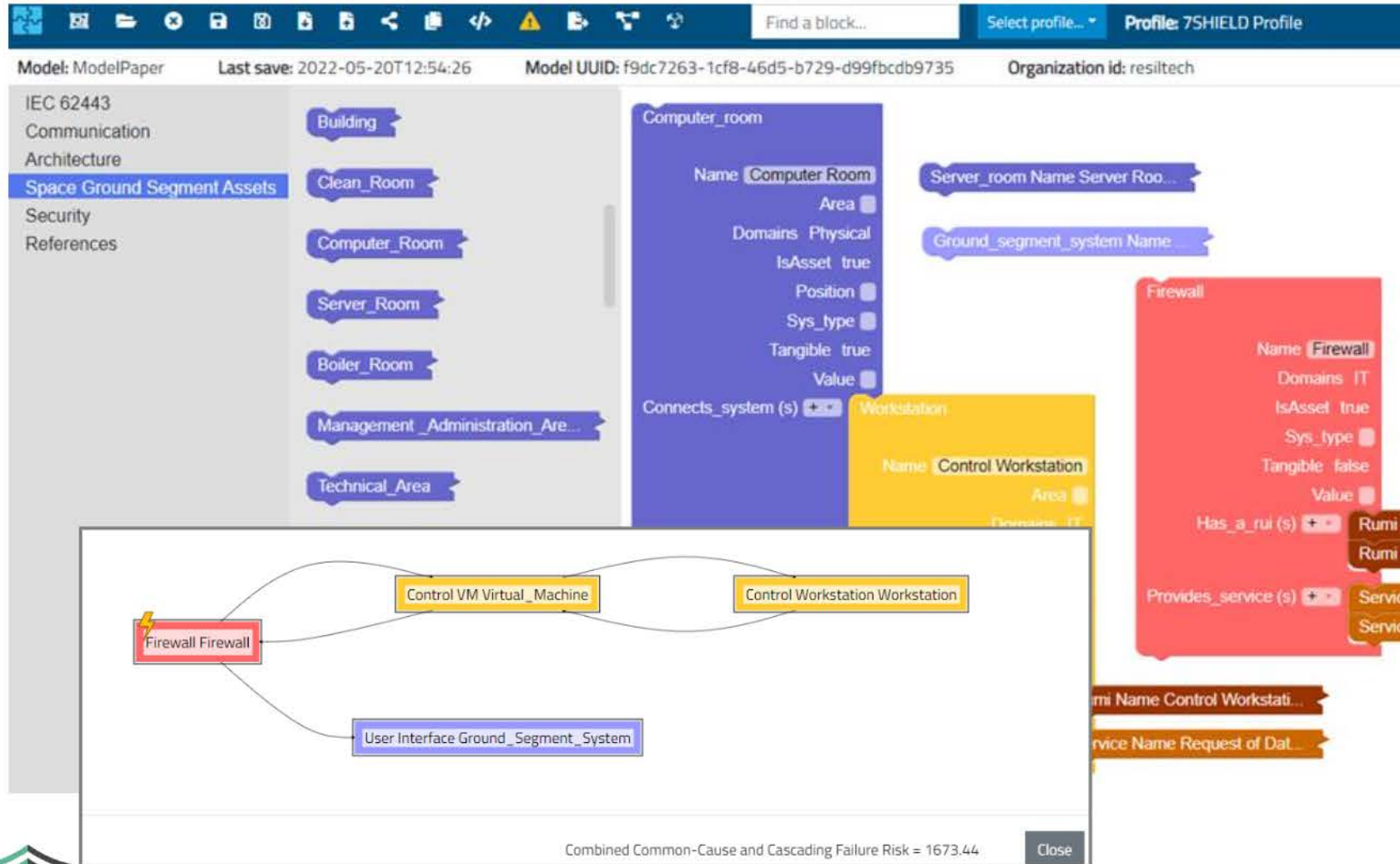


The model of the infrastructure of Ground Segment systems guide the analysis of the system in order to verify security properties

Automatic support for keyword-based vulnerability analysis has been exploited with the aim to perform a complete and effective analysis of all possible cascading path for malicious (and accidental) system failure



# Model Based Design and Assessment Tool



7SHIELD Profile used for

- modelling the overall system infrastructure considering its hierarchical decomposition
- identifying both cyber and physical interfaces for each component for each level of abstraction
- guiding the analysis of cascading effects






# Cyber and Physical Threat Intelligence

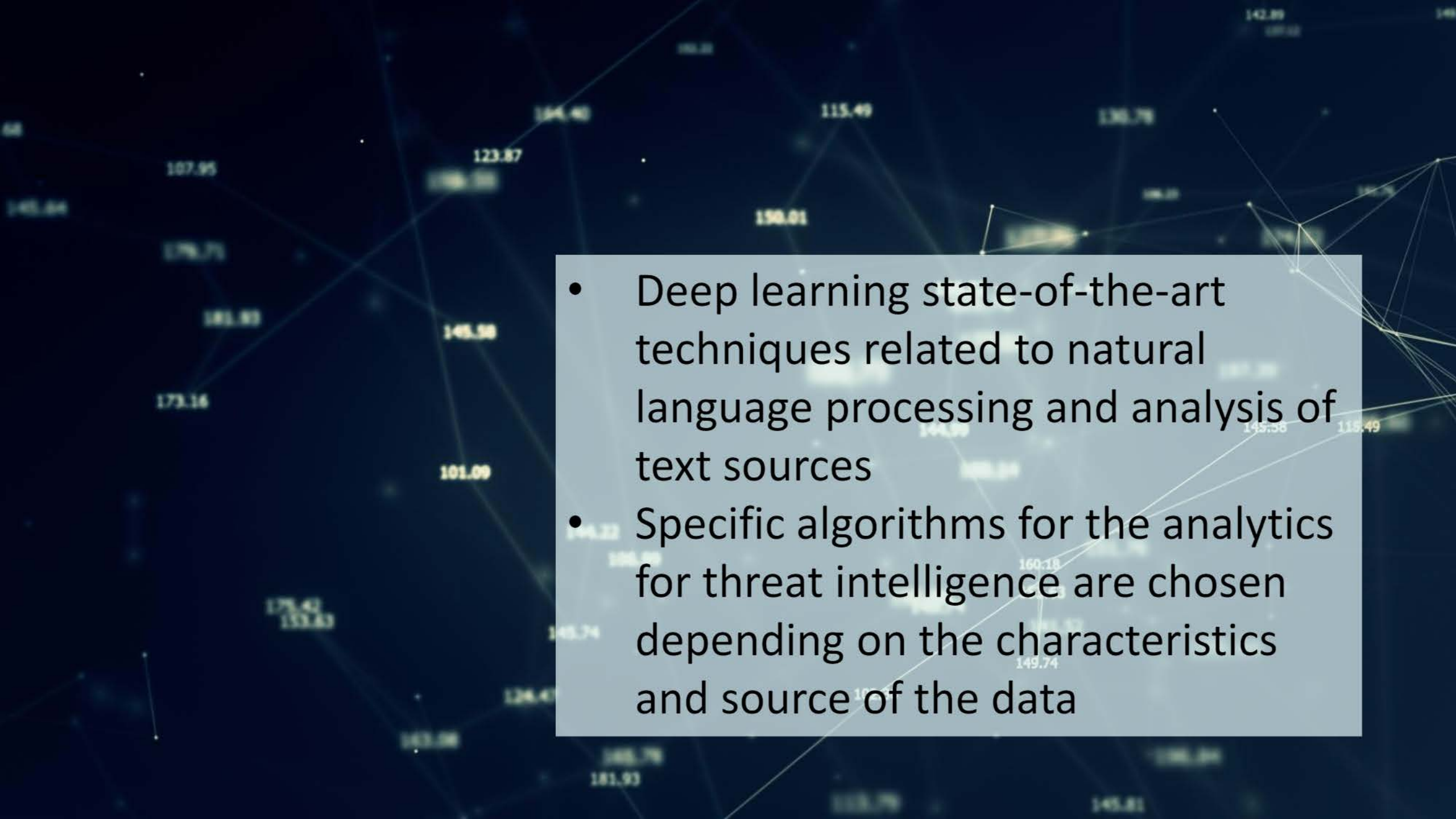
Identification, collection and analysis of cyber and physical threat intelligence data based on open source feeds and commercial providers

Knowing potential external threats on the critical infrastructure will raise the level of vigilance



A large crowd of diverse people, seen from a high angle, is arranged to form the geographical shape of the European continent. The individuals are dressed in various casual and business-casual attire, creating a mosaic of colors. The background is a plain, light-colored surface.

Retrieve information from  
social networks, forums,  
blogs on the surface, deep  
and dark web to identify  
possible threats coming from  
Open Source Intelligence  
(OSINT) data

- 
- Deep learning state-of-the-art techniques related to natural language processing and analysis of text sources
  - Specific algorithms for the analytics for threat intelligence are chosen depending on the characteristics and source of the data





7SHIELD

*Thank You*

<https://www.7shield.eu/>



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



# Crisis management

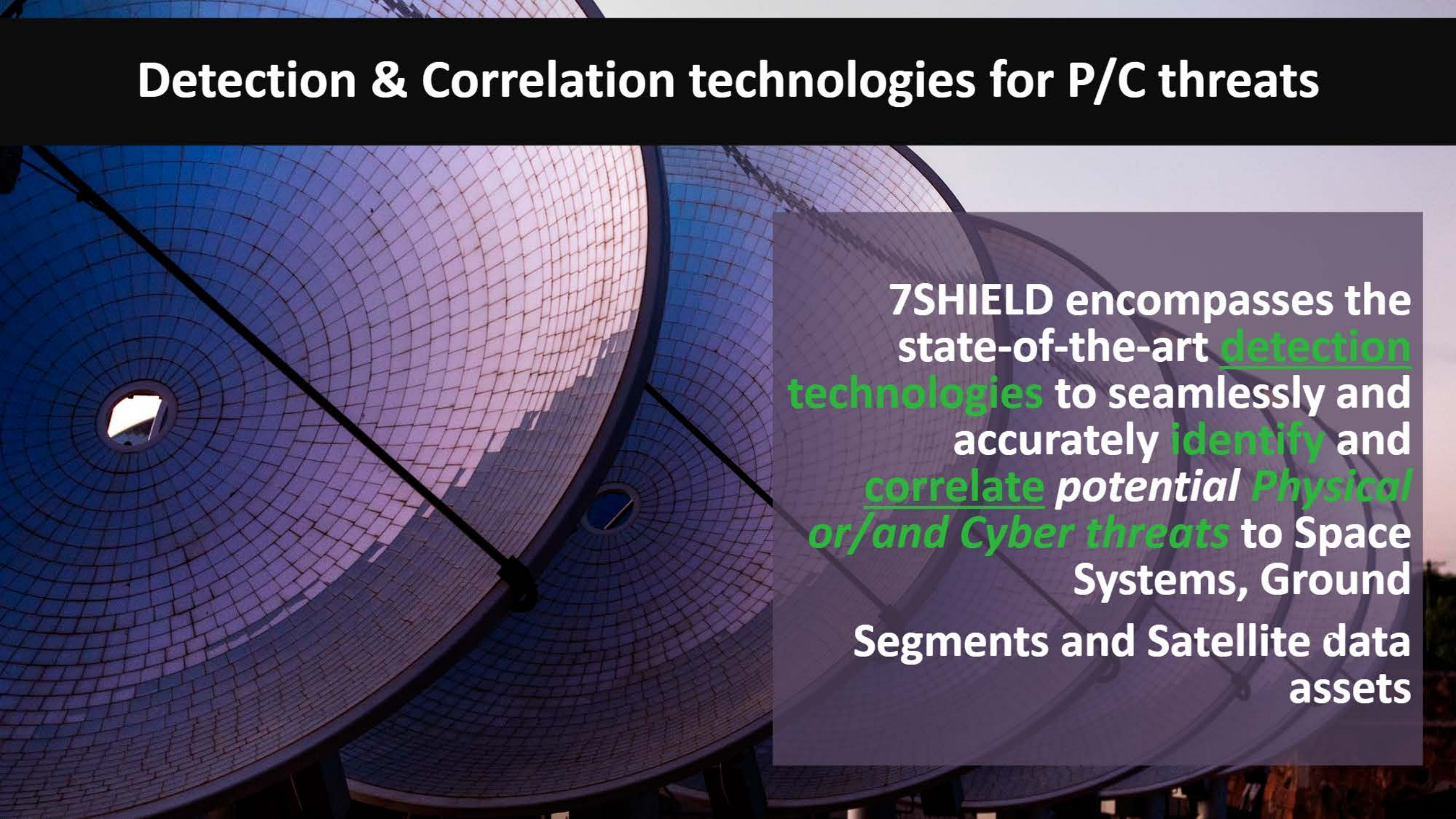
Gerasimos Antzoulatos (CERTH)

WP4 leader



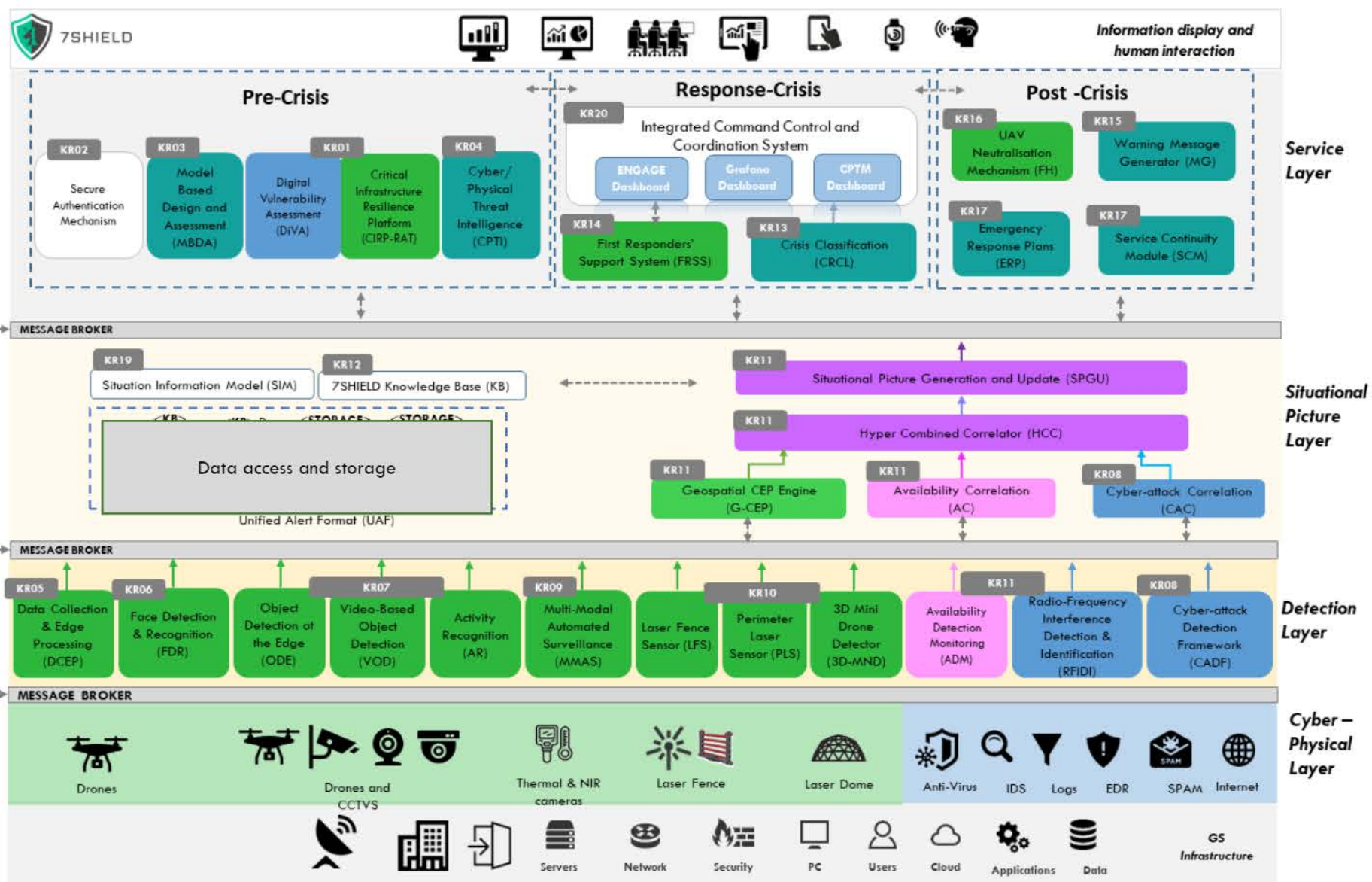


# Detection & Correlation technologies for P/C threats



7SHIELD encompasses the state-of-the-art detection technologies to seamlessly and accurately identify and correlate *potential Physical or/and Cyber threats* to Space Systems, Ground Segments and Satellite data assets





**7SHIELD**



# Data collection and edge processing module



A dedicated Payload Management system allows **quick plug-and-play hardware re-configuration**, so that **different sensor payloads** can be **installed on-board** the UAVs depending on the specific operation needs





## The *Data Collection and Edge Processing (DCEP)* supports:

- on board processing
  - ✓ embed an edge processor able to host **advanced AI algorithms**
  - ✓ **object detection and identification** services
- **communication capabilities** with the control room
- basic drone functions such as
  - **autonomous flights**
  - **camera synchronization**
  - **locating objects during the flight**





# Face detection and face recognition module

Encompass state-of-the-art methodologies for **optical video surveillance** and **extract high-level information** from any single image shot and/or video streams



**FDR processes live video streams** from Close Circuit Television (CCTV) cameras, in order to warn about **detected faces** that may **belong to unauthorised individuals**.

The module **produces alarms** whenever a **detected face cannot be matched** with any person from the **authorised-person database** (which contains image data of individuals that have authorization to move into the monitored area).





# Video-based Object Detection and Activity Recognition module

A white, bullet-style security camera is mounted on a wall made of grey rectangular tiles. The camera is angled downwards and to the right. It has a black lens in the center, surrounded by several small, circular infrared LEDs. The mounting bracket is white and has two screws visible on the wall.

Integrate the capacity of enhanced detection to:  
**detect, identify and track objects of interest,**  
**recognise activities and**  
**extract multimedia concept from surveillance cameras**



**Video-based Object Detection (VOD)**  
and **Object Detection at the Edge (ODE)**  
recognize and identify all objects of  
interest depicted in the provided input  
video (or video stream)

**Activity Recognition (AR)** module  
detects any potential suspicious activity  
performed by the human subjects that  
have been detected

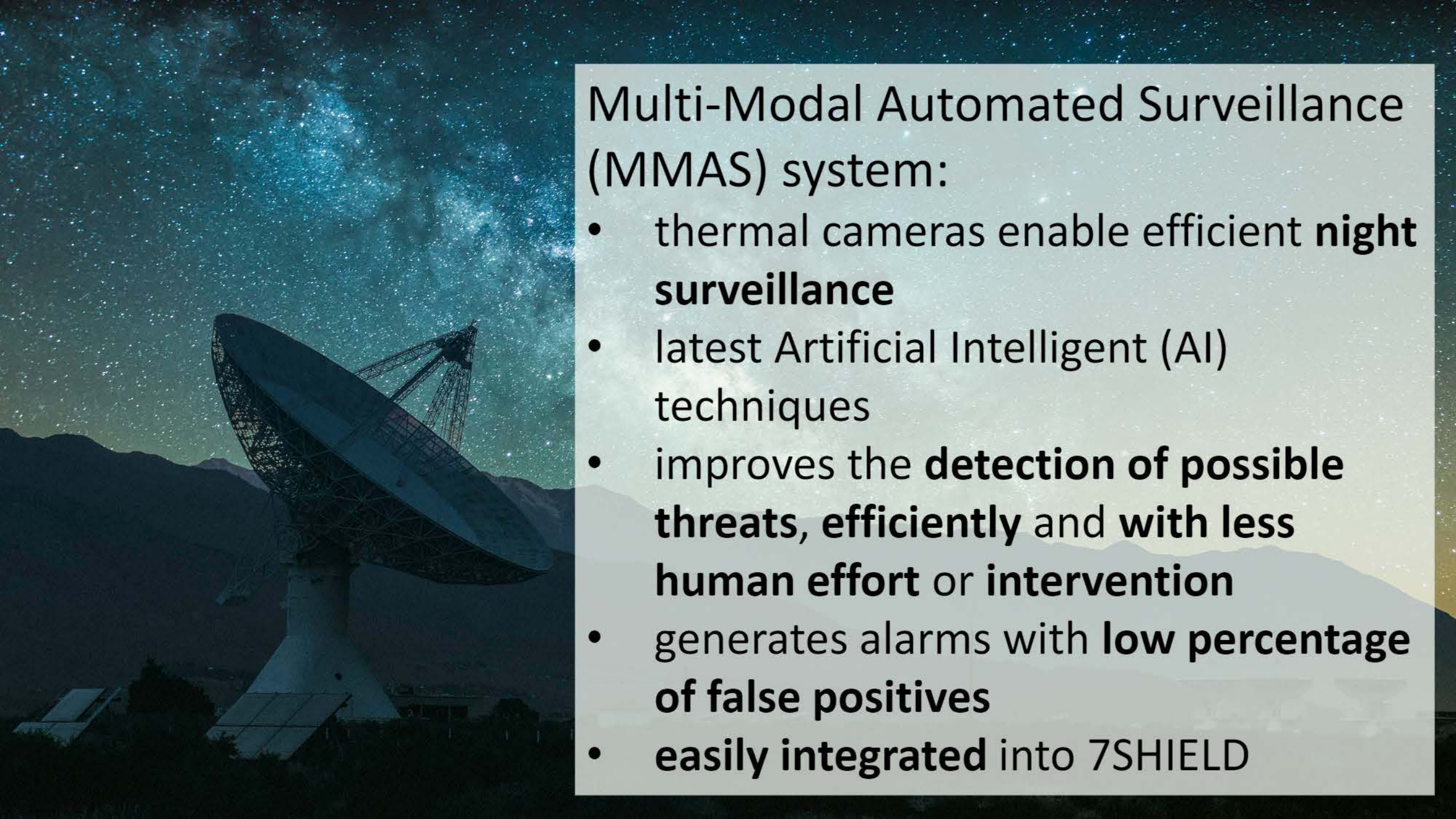


The image is a composite of four thermal and near-infrared (NIR) surveillance frames. The top-left frame shows a person in a hooded jacket with a temperature reading of 15.4. The top-right frame shows a person's face with a temperature reading of 15.9. The bottom-left frame shows a person's head and shoulders with a temperature reading of 34.5. The bottom-right frame shows a person's face with a temperature reading of 36.0. A color scale bar is visible on the right side of each frame, ranging from blue (cooler) to red (warmer).

# Thermal and near-infrared image processing for man-made threats

The development of a *Multimodal Automated Surveillance (MMAS)* system to detect the presence of intruders, such as moving objects and people, within the boundaries of an area under surveillance

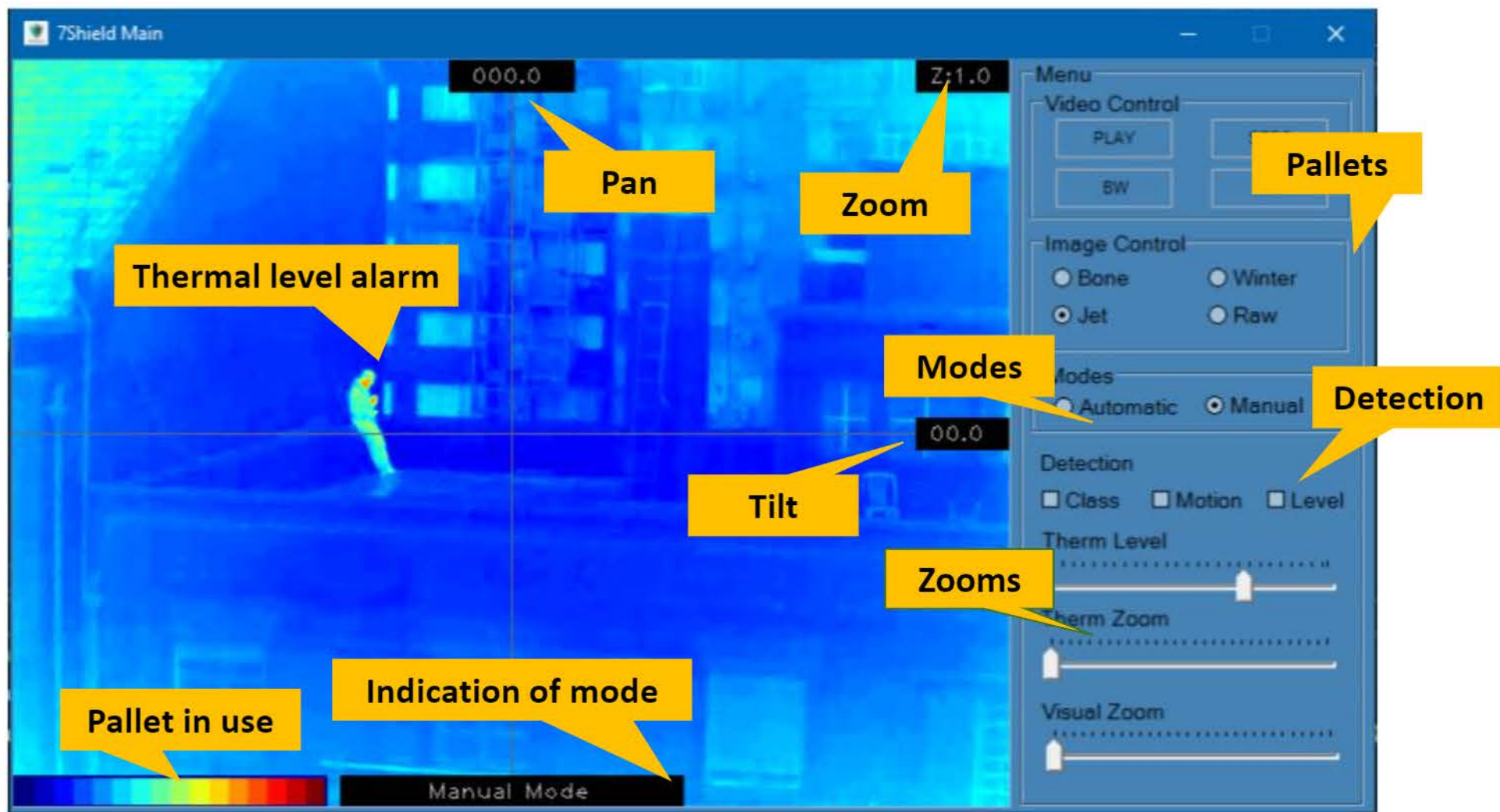




## Multi-Modal Automated Surveillance (MMAS) system:

- thermal cameras enable efficient **night surveillance**
- latest Artificial Intelligent (AI) techniques
- improves the **detection of possible threats, efficiently** and **with less human effort** or **intervention**
- generates alarms with **low percentage of false positives**
- **easily integrated** into 7SHIELD





Thermal raw image



Thermal image with classification alarms

MMAS User Interface in Manual mode



7SHIELD

7SHIELD



# Detection of ground based and aerial intruders

The background image shows a person in silhouette standing on a platform, looking out over a bright, hazy horizon. A large, glowing light source, possibly the sun, is visible in the center of the horizon, creating a strong backlight effect. The sky is filled with soft, hazy clouds, and the overall color palette is dominated by warm, orange and yellow tones.

Innovative laser-based detection  
system is to be used for detection  
of ground based and aerial  
intrusion





*Perimeter Laser Sensor V3.0 (PLS)*  
*and Laser Fence Sensor V3.0 (LFS)*  
for **ground level intrusion**  
**detection** against humans and  
vehicles;

*3-Dimensional Mini Drone*  
*Detector V3.0 (3D MND)* for  
detection of **intrusion by mini**  
**drones in the air** space above  
infrastructure sites



A close-up, low-key photograph of a person's face, focusing on their eyes behind glasses. The image is heavily stylized with a teal/cyan color cast. Overlaid on the lenses of the glasses is a pattern of white binary code (0s and 1s), suggesting a digital or cyber theme. The person's face is partially in shadow, and the background is dark.

# Cyber-attack detection framework

**Collection of information at several architectural levels (namely: Network, Operating System, Data Base, Application, and Business Process) and use of sophisticated data analysis techniques for cyber-attack detection**





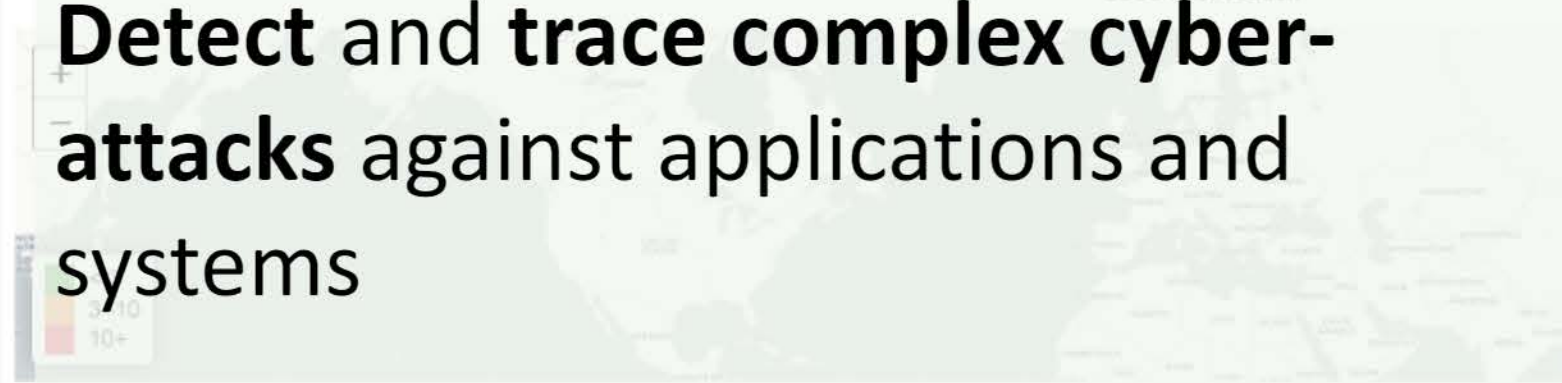
Filters Filters Filters

**Detect and trace complex cyber-attacks** against applications and systems

Heterogeneous security probes

Events are processed, analytics on the status of the system are provided and alerts are raised in case of incoming cyber-attacks

DDoS GeoLocation



Last 5 minutes

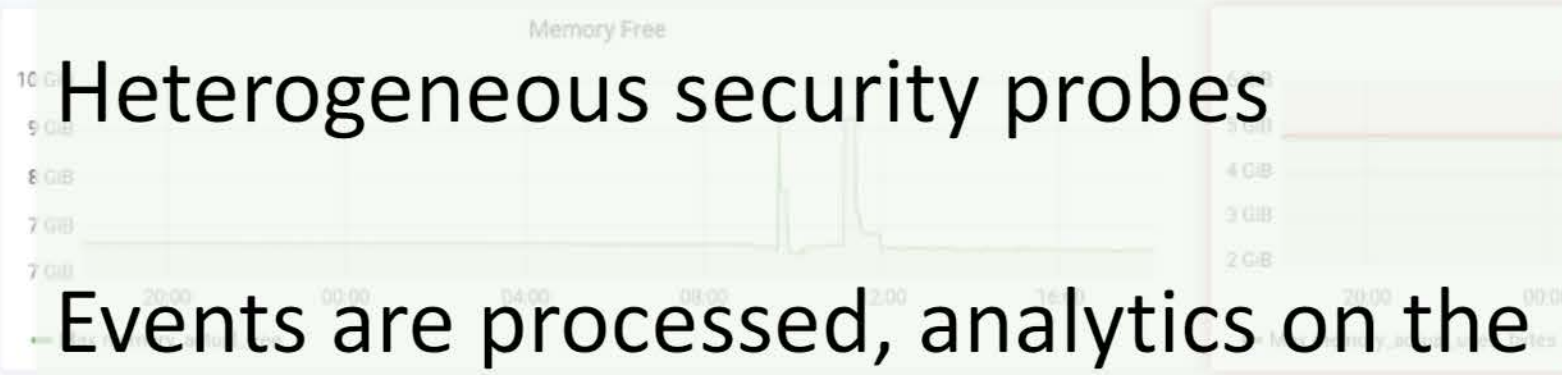


Leaflet | © OpenStreetMap © CartoDB

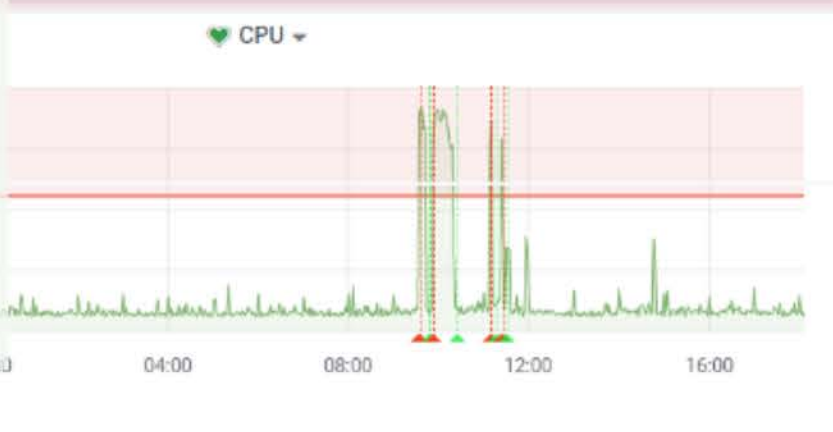
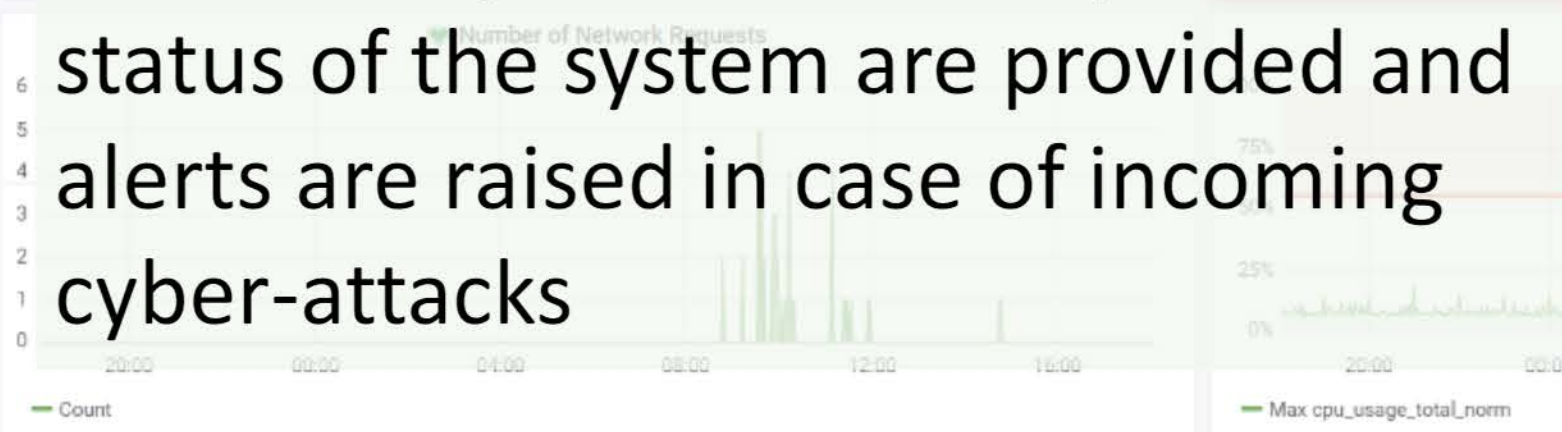
2022-09-28 08:06:00

Max cpu\_usage\_total\_norm: 19%

Memory Used



CPU





SIEM Rule Designer

Designer

Nodes

Source

Filter

Count

Join

Enrich

Union

Chain

Timer

Output

Functions

Render

Clears

Refresh Srcs

Import project

Animations

Network\_IDS\_Events

Out

DDoS\_Detection\_Filter

In

Out

Correlation

In

Out

Correlated\_Events

In

Ip\_Blacklists

Out

join

Node Name : Correlation

Delete

Delete Out Links

Note

Time props

Fields 1th source : DDoS\_Detection\_Filter

✓ alert->signature

✓ alert->category

✓ alert->severity

✓ alert->signature\_id

✓ host

✓ event\_type

✓ dest\_port

✓ type

✓ path

✓ proto

✓ src\_ip

✓ src\_port

✓ dest\_ip

Match field 1 : src\_ip

Fields 2nd source: Ip\_Blacklists

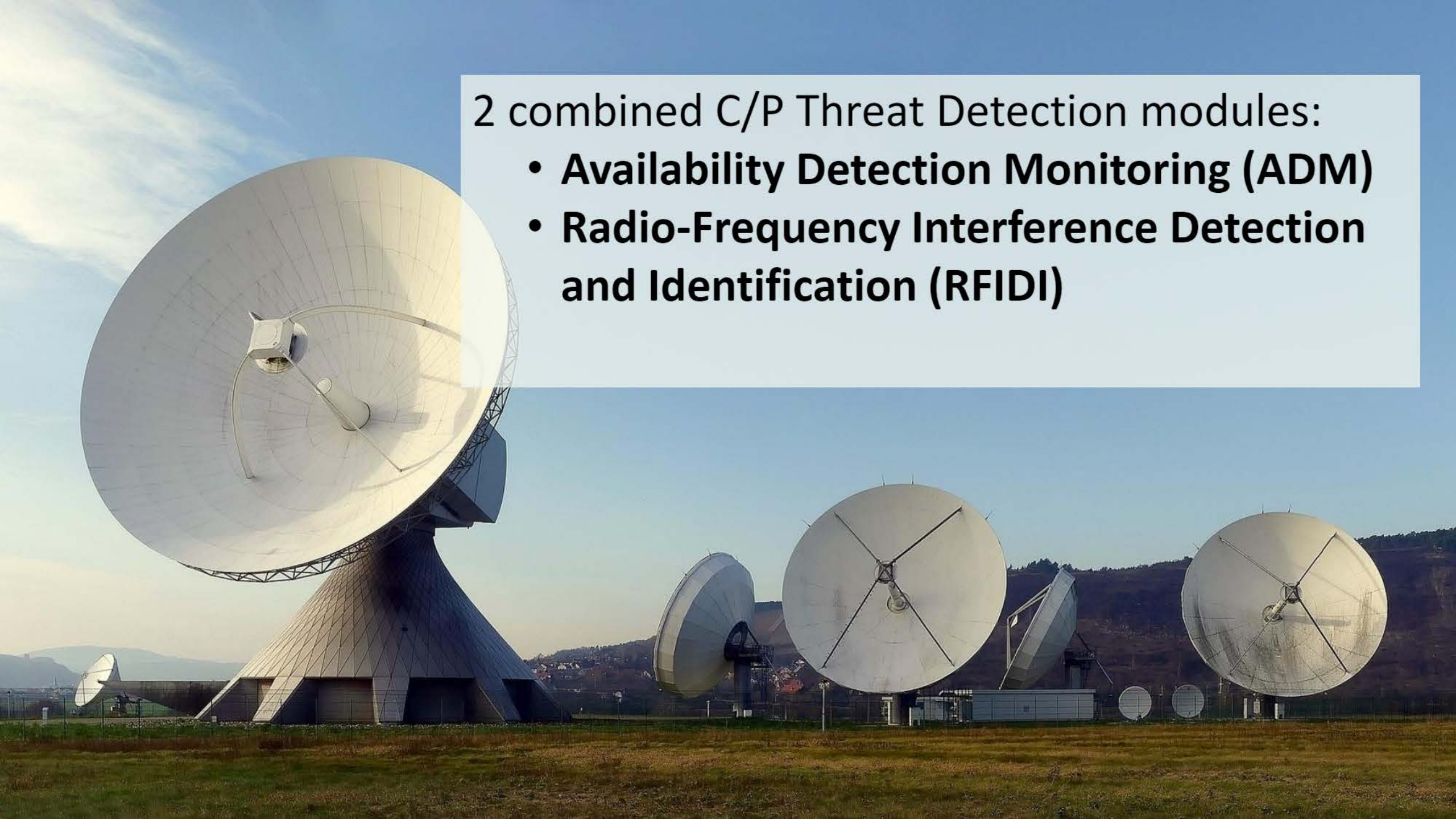
✓ crowdsec\_event->ip

✓ crowdsec\_event->event

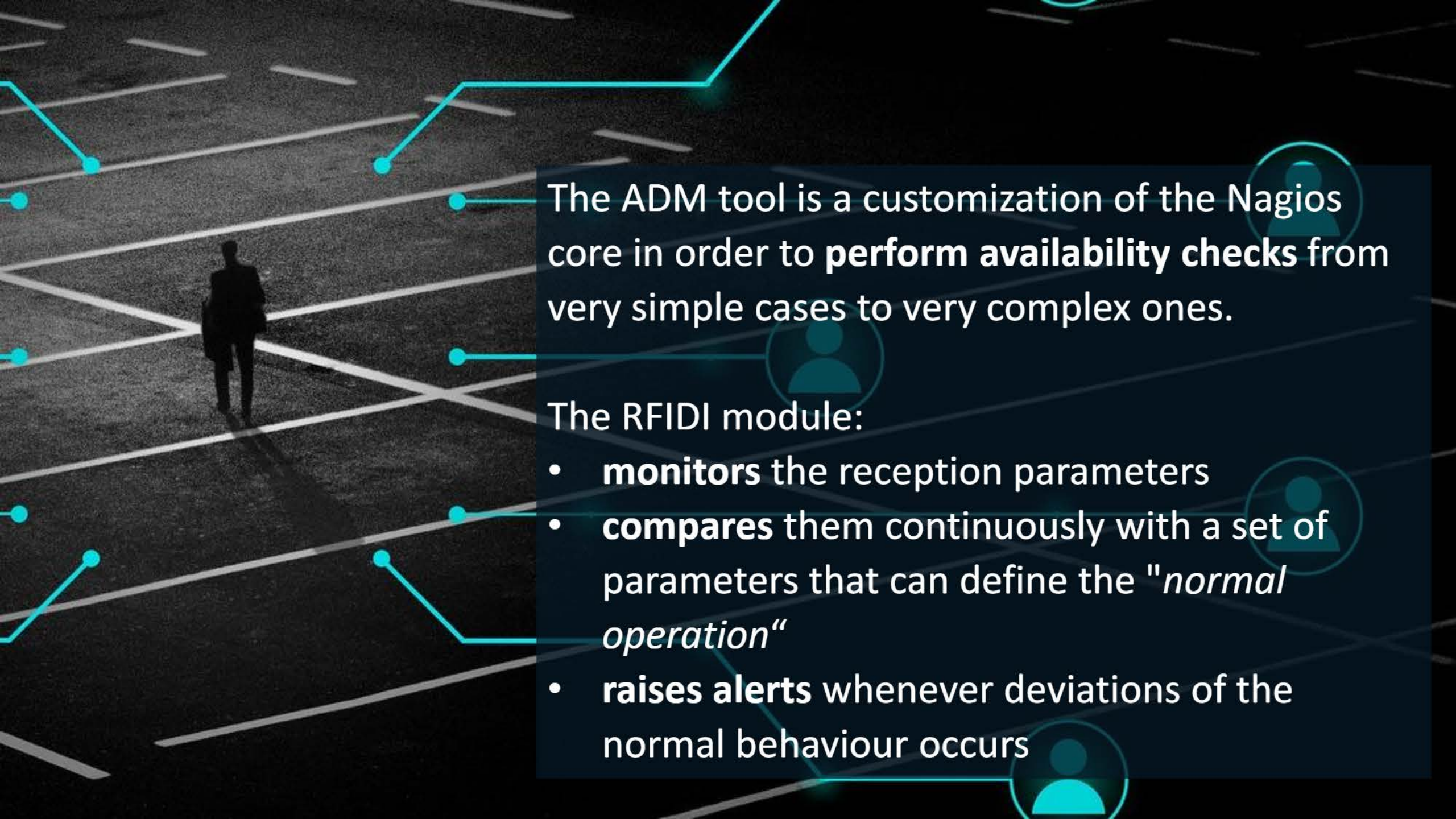
Match field 2 : crowdsec\_event->ip

The data are collected by the probes and correlated through pre-defined rules using open-source software tools



- 
- 2 combined C/P Threat Detection modules:
- **Availability Detection Monitoring (ADM)**
  - **Radio-Frequency Interference Detection and Identification (RFIDI)**





The ADM tool is a customization of the Nagios core in order to **perform availability checks** from very simple cases to very complex ones.

The RFID module:

- **monitors** the reception parameters
- **compares** them continuously with a set of parameters that can define the "*normal operation*"
- **raises alerts** whenever deviations of the normal behaviour occurs



# Combined C/P Threat Detection and Early Warning module

Processes for detection and early warning already exist in Cyber Threat Detection but they are usually designed to work on a single type of data

Those processes are improved in 7SHIELD to **work on multiple type of data simultaneously** so to identify **multi-data complex scenarios** or **multi-data weak signals** or **abnormal behavior**





## **Event correlator tools:**

- **Geospatial Complex Event Processing Engine (G-CEP)**
- **Availability Correlator (AC)**
- **Hyper Combined Correlator (HCC)**
- **Situational Picture Generation and Update (SPGU)**





7SHIELD

*Thank You*

<https://www.7shield.eu/>



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





# Postcrisis management

Paulo Chaves (INOV)  
WP5 Leader





# Response & Mitigation technologies for physical and cyber threats

**In 7SHIELD the innovative technologies are tailored to monitor the evolvement of a physical or/and cyber-attacks, to strengthen the responsiveness and social awareness**

**The appropriate actions to mitigate the consequences of physical and cyber-attacks, focusing on the services continuity, are consolidated**

A large, red, stylized graphic on the right side of the slide. It features a triangular warning symbol at the top, followed by the words "SECURITY" and "ALERT" in a bold, sans-serif font. The background of this graphic is a dark red circle with a gear-like or radar-like pattern around the perimeter. The overall theme is cybersecurity and emergency response.

**SECURITY  
ALERT**



## Response

Semantic reasoning

Crisis level classification

Decision support system

Social awareness

Intruding UAV neutralization

## Mitigation

Service continuity

Emergency response

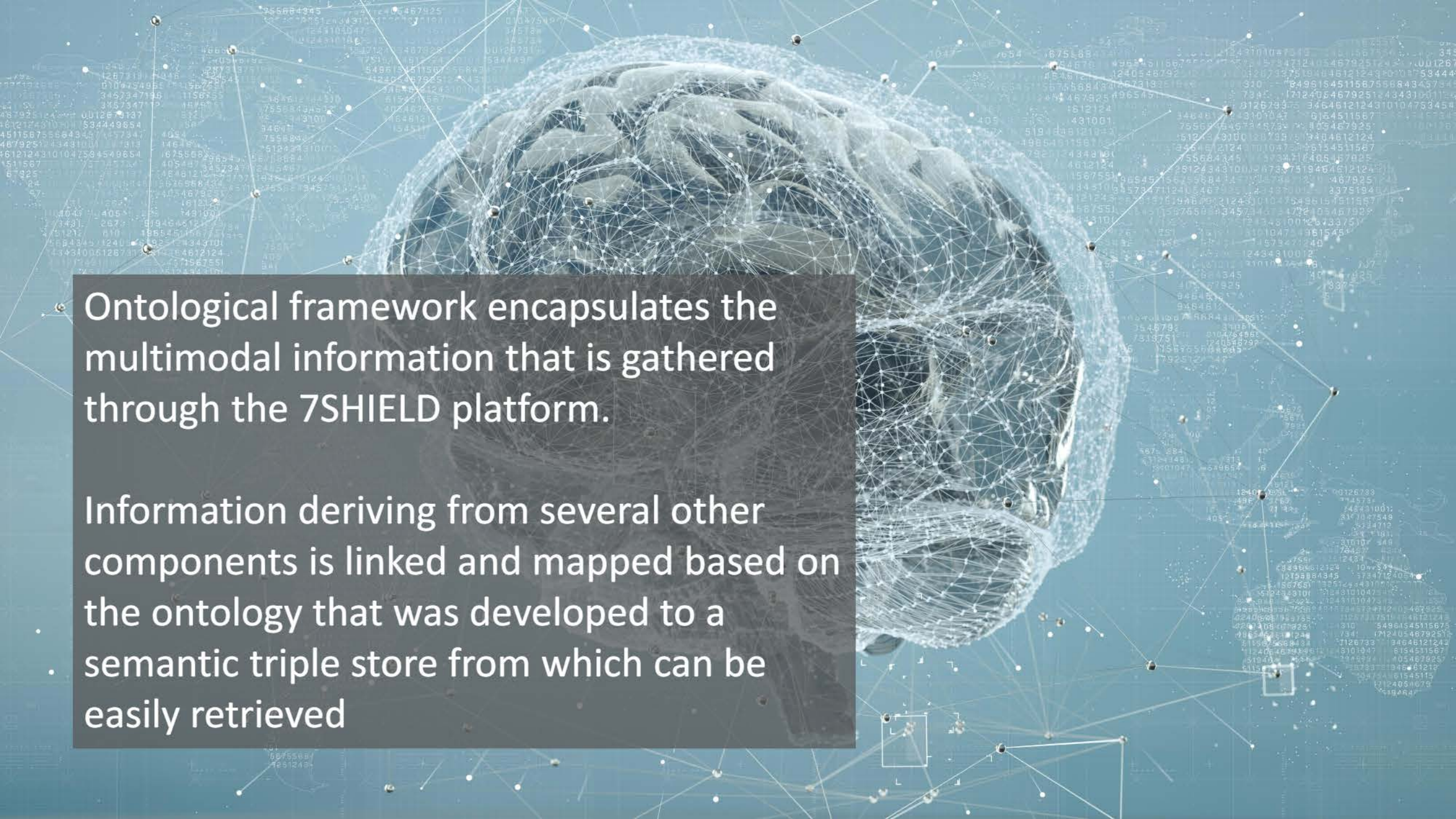


# 7SHIELD Knowledge Base

Efficient semantic model for representing data pertinent to 7SHIELD:

- (a) personal data (eg. face and person recognition, user profile),
- (b) time and location information,
- (c) weather information,
- (d) concepts identification information,
- (e) object detection information,
- (f) event extraction information and (g) sensors information, which derive from satellite data, sensors and 7SHIELD tools





Ontological framework encapsulates the multimodal information that is gathered through the 7SHIELD platform.

Information deriving from several other components is linked and mapped based on the ontology that was developed to a semantic triple store from which can be easily retrieved



## Process

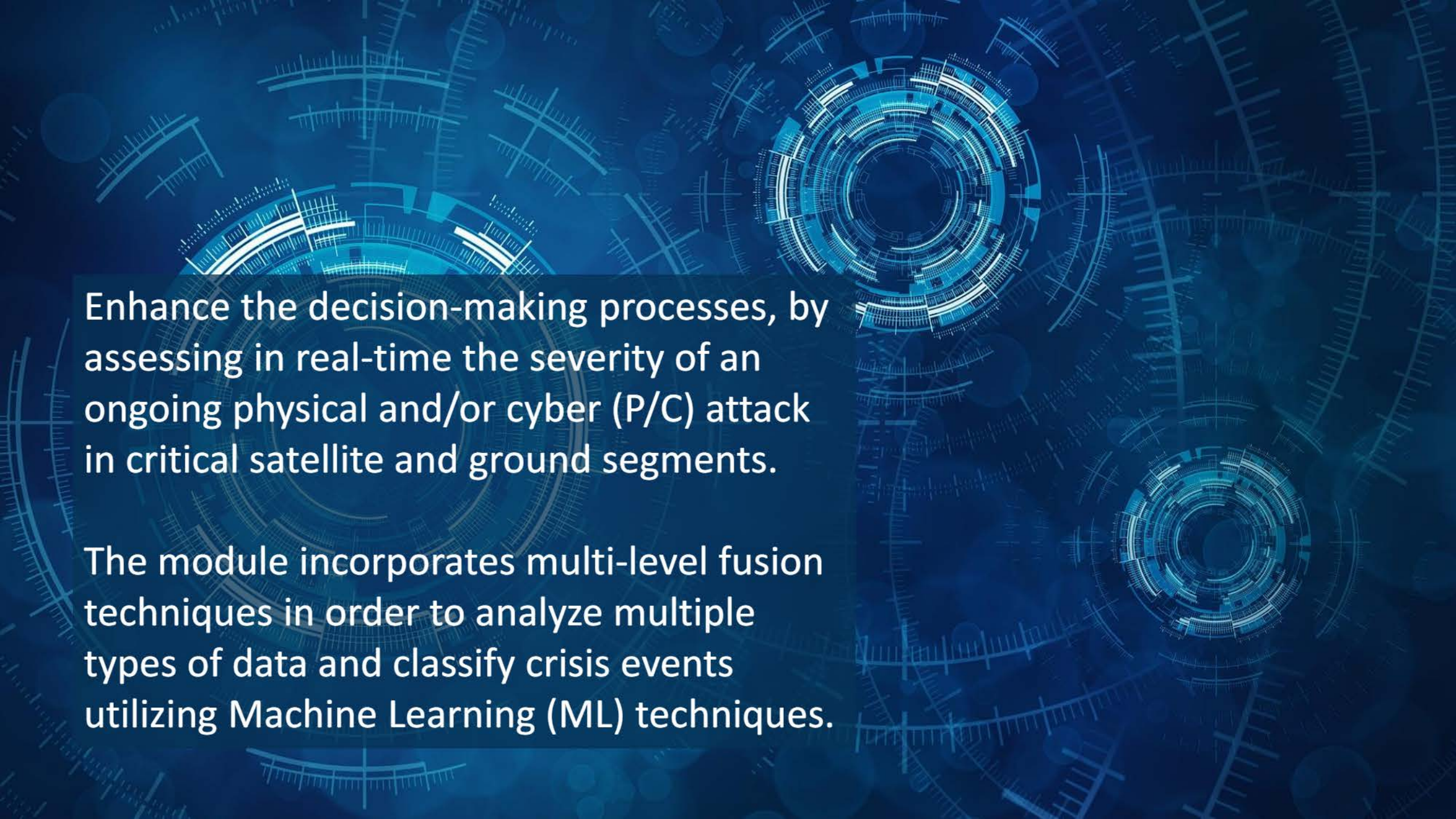
- Selection of an upper-level ontology
- Study of the state-of-the-art domain ontologies (SOSA / SSN)
- Creation of population service (use of semantic library RDF4J) to match all the incoming information to a triple store
- Use of SPARQL queries.



# **Crisis Classification (CRCL) Module**

Assess robustly the severity of an ongoing physical and/or cyber-attack and classify it into pre-defined categories.






Enhance the decision-making processes, by assessing in real-time the severity of an ongoing physical and/or cyber (P/C) attack in critical satellite and ground segments.

The module incorporates multi-level fusion techniques in order to analyze multiple types of data and classify crisis events utilizing Machine Learning (ML) techniques.





7SHIELD pilot contributed to create annotated datasets to train ML models for assessing the severity level of an ongoing P/C attack.

CRCL runs in a Docker container as a back-end process, making it easy to deploy and operate on any platform





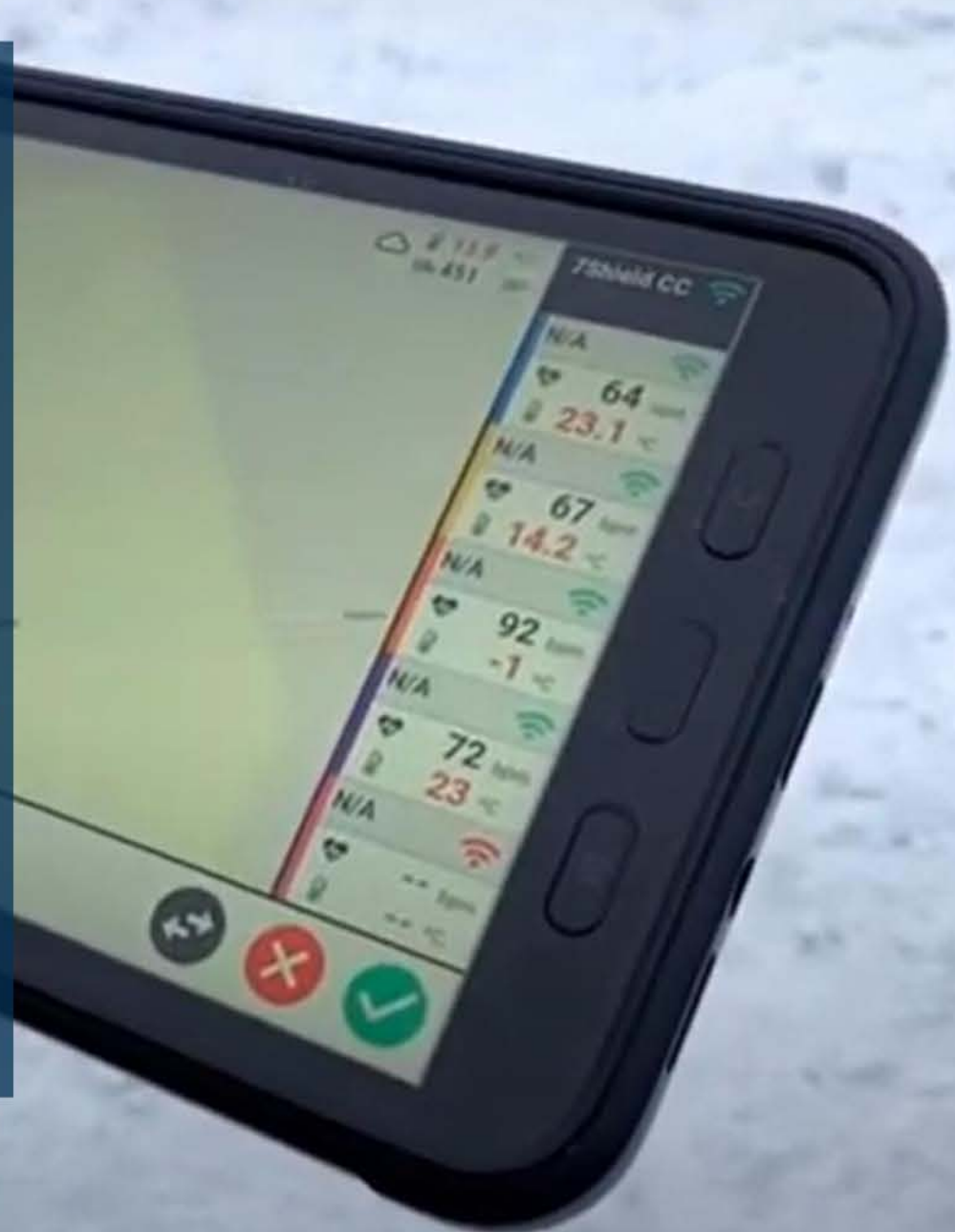
# Tactical Decision Support System (TDSS)

Encompass evidence-based decision-making tools to facilitate decision makers and authorities in their mission to face emergency response

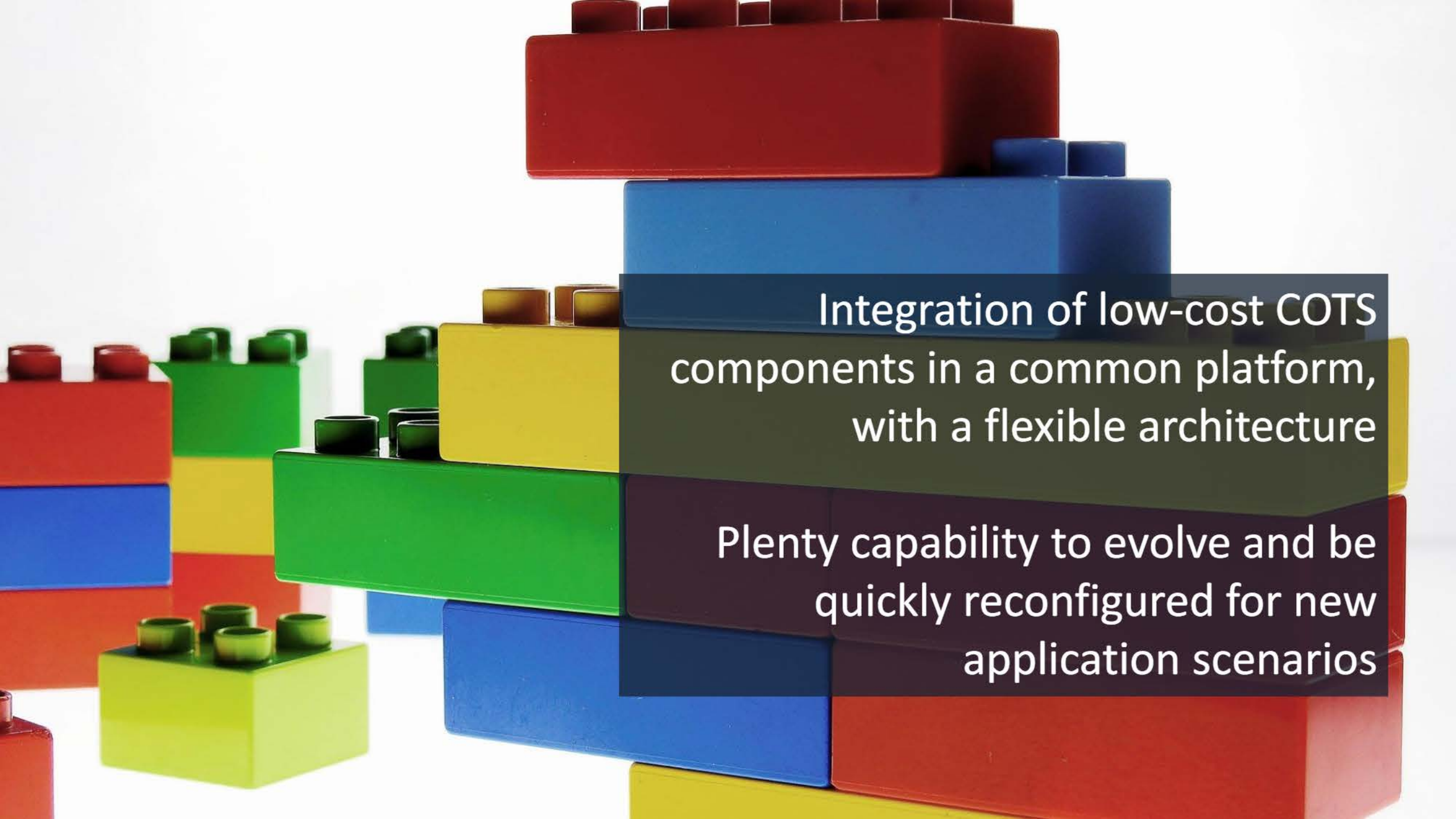


- Wearables sensors,
- Communication transceivers
- Universal Tactical Display (UTD) for action team members.

The use of a TDSS First Responder teams enables teams to be self-aware and have more information to support effective decision making in the field even without an infrastructure or Command and Control center(C2) support





A stack of colorful building blocks (red, blue, yellow, green) is shown against a white background. The blocks are arranged in a stepped fashion, with some blocks having small protrusions on top. Two semi-transparent text boxes are overlaid on the right side of the stack.

Integration of low-cost COTS  
components in a common platform,  
with a flexible architecture

Plenty capability to evolve and be  
quickly reconfigured for new  
application scenarios

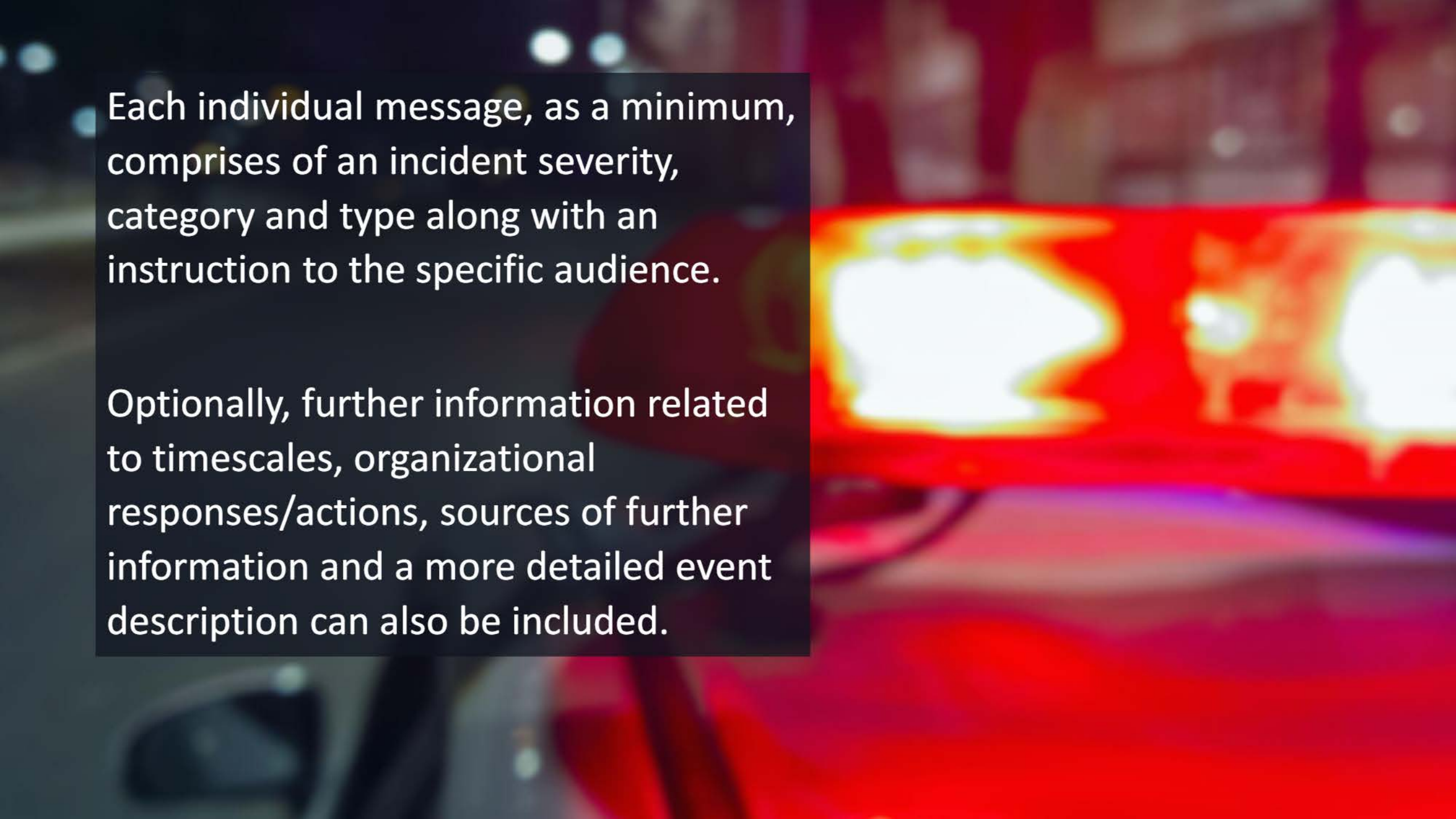




# **Social Awareness and Warning Message Generation**

Social Engagement guidelines in using social media for maximum impact in emergency situation providing informative practical guidance to affected communities





Each individual message, as a minimum, comprises of an incident severity, category and type along with an instruction to the specific audience.

Optionally, further information related to timescales, organizational responses/actions, sources of further information and a more detailed event description can also be included.



## Warning Message Generation

Language

English

Severity

Red

Override ☐

Message Type

alert

Override ☐

Category

trespasser on site (single person)

Override ☐

Red alert for trespasser on site (single person) active from now until further notice at the ground station. Employees should stay indoors. Security is investigating. Update expected at 16:00 Visit [www.7shield.eu](http://www.7shield.eu) for more information. Contact us on 777.

Copy

Simple form in a web-based application that allows the user to build up their message through the various pre-filled content blocks

Message templates and content blocks are fully customizable and could be deployed to adapt to any type of organization or incident



7SHIELD

7SHIELD



# UAV neutralisation mechanism



Innovative methods of neutralisation of the intruding drones: intruding drone will be physical “caught” by an operator controlled / autonomous drone, which brings the intruder drone to a designated spot





Flying  
Hunter

Net

mini drone captured using under-belly net and  
brings it to a predetermined location on the  
ground and drops it there





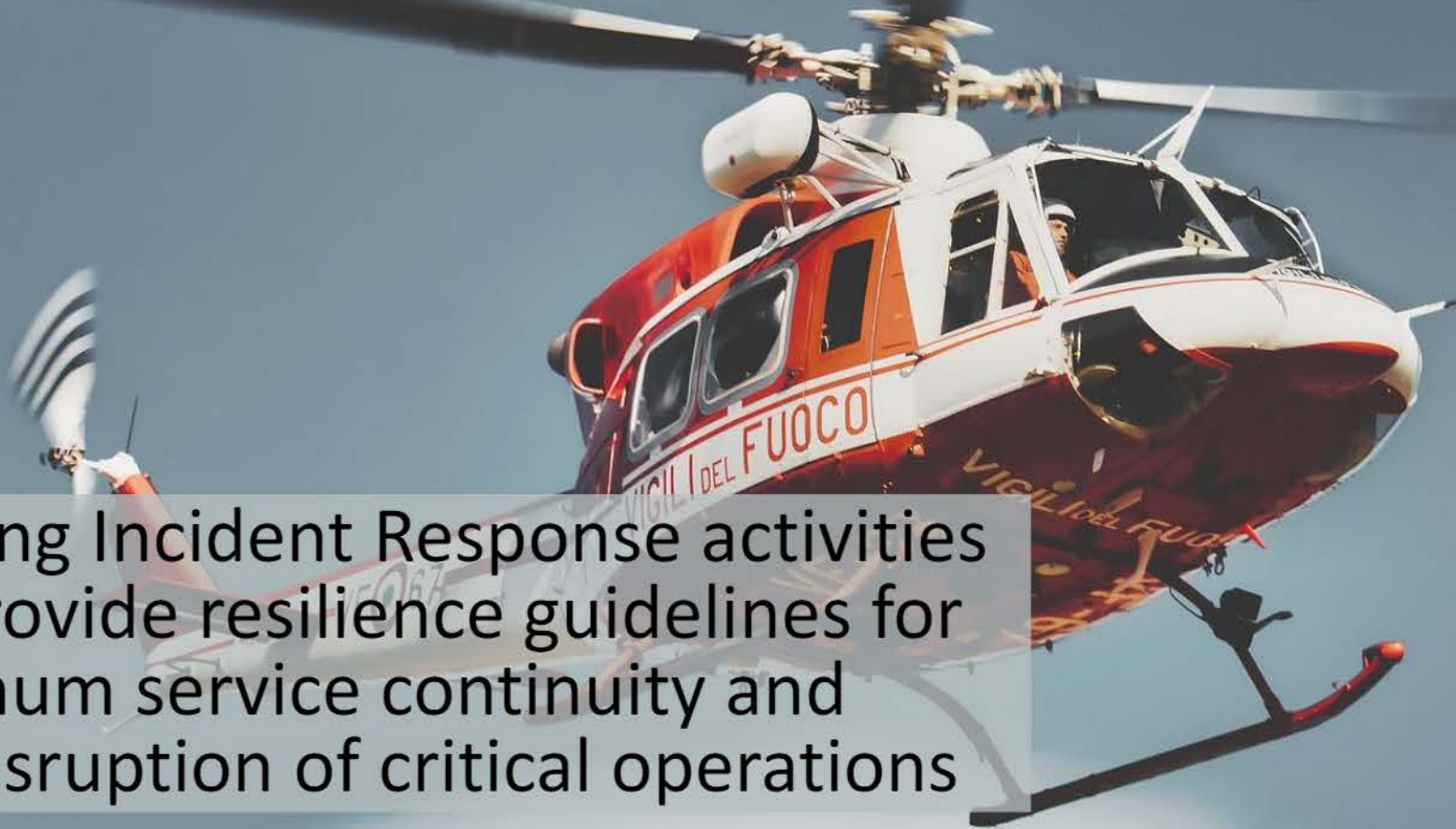
This way, mini drone can be carried out as the mini drone is not destroyed

Bringing it to the predesignated location on the ground, forensic analysis of the intruder are enabled



# Potential impacts from C/P attacks and countermeasures knowledge base

Planning Incident Response activities and provide resilience guidelines for maximum service continuity and non-disruption of critical operations






The background of the slide features a blurred image of emergency vehicle lights, with prominent blue and red streaks and bokeh effects, suggesting a scene of an emergency response.

## Emergency Response Plan module

provides a set of specific, self-standing operational playbook in a form of on-screen instructions tailored to the local GS

enables the efficient and successful management of an incident in a structured and comprehensive way by guiding the operators performing specific tasks and actions during an emergency..

A person in a dark suit is seen from behind, standing in a modern office and looking out a large window at a city skyline. The scene is dimly lit, with the primary light source being the window. A semi-transparent text box is overlaid on the right side of the image.

The **Service Continuity Module** allows to perform a failure propagation analysis and rapid assessment of a real or hypothetical disaster scenarios, selecting several physical/cyber (p/c) attacks per component or downtimes



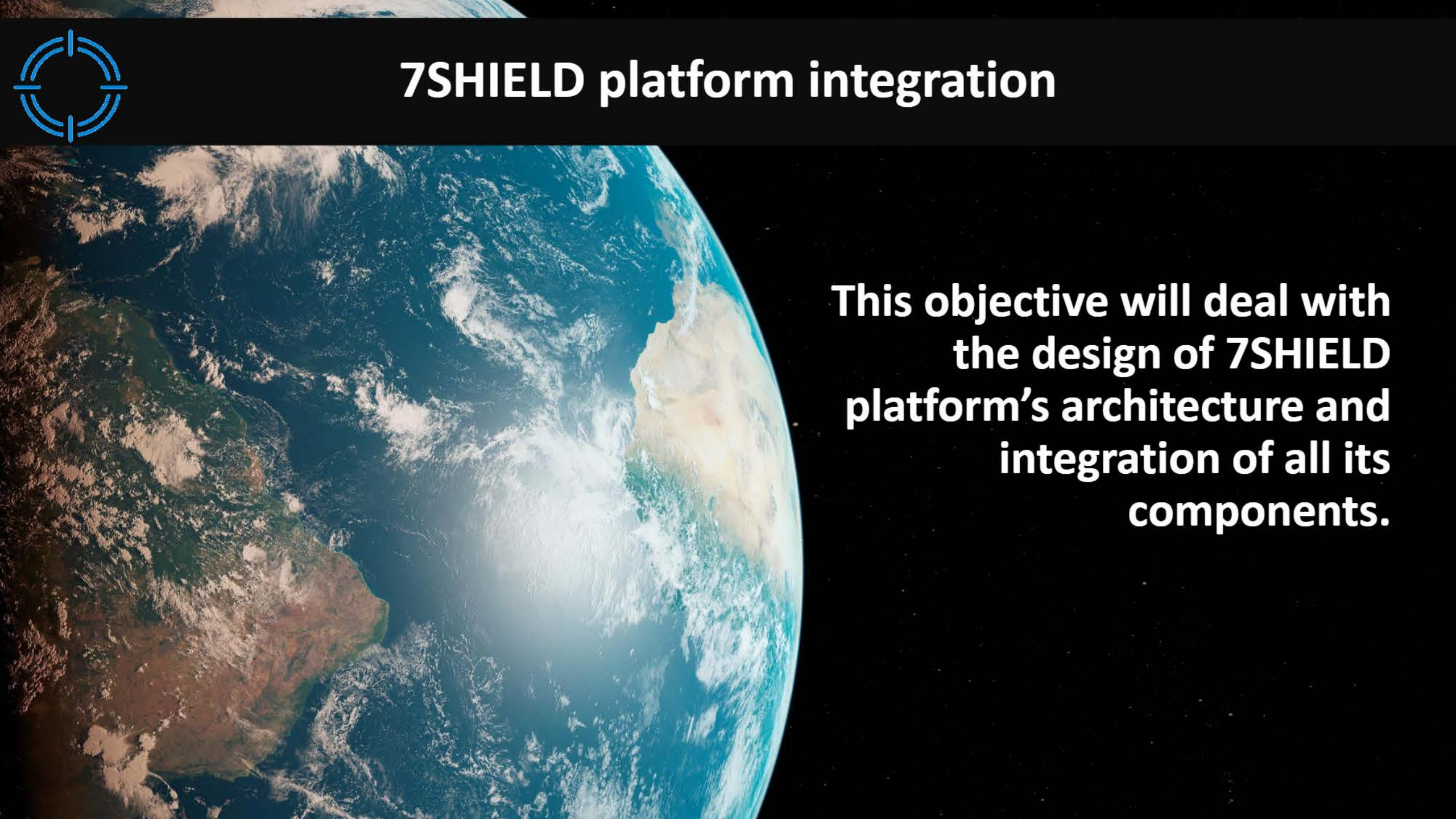


## 7SHIELD platform

Carmen Stira , Francesco Durante (ENG)  
WP6 Leader







# 7SHIELD platform integration

**This objective will deal with the design of 7SHIELD platform's architecture and integration of all its components.**



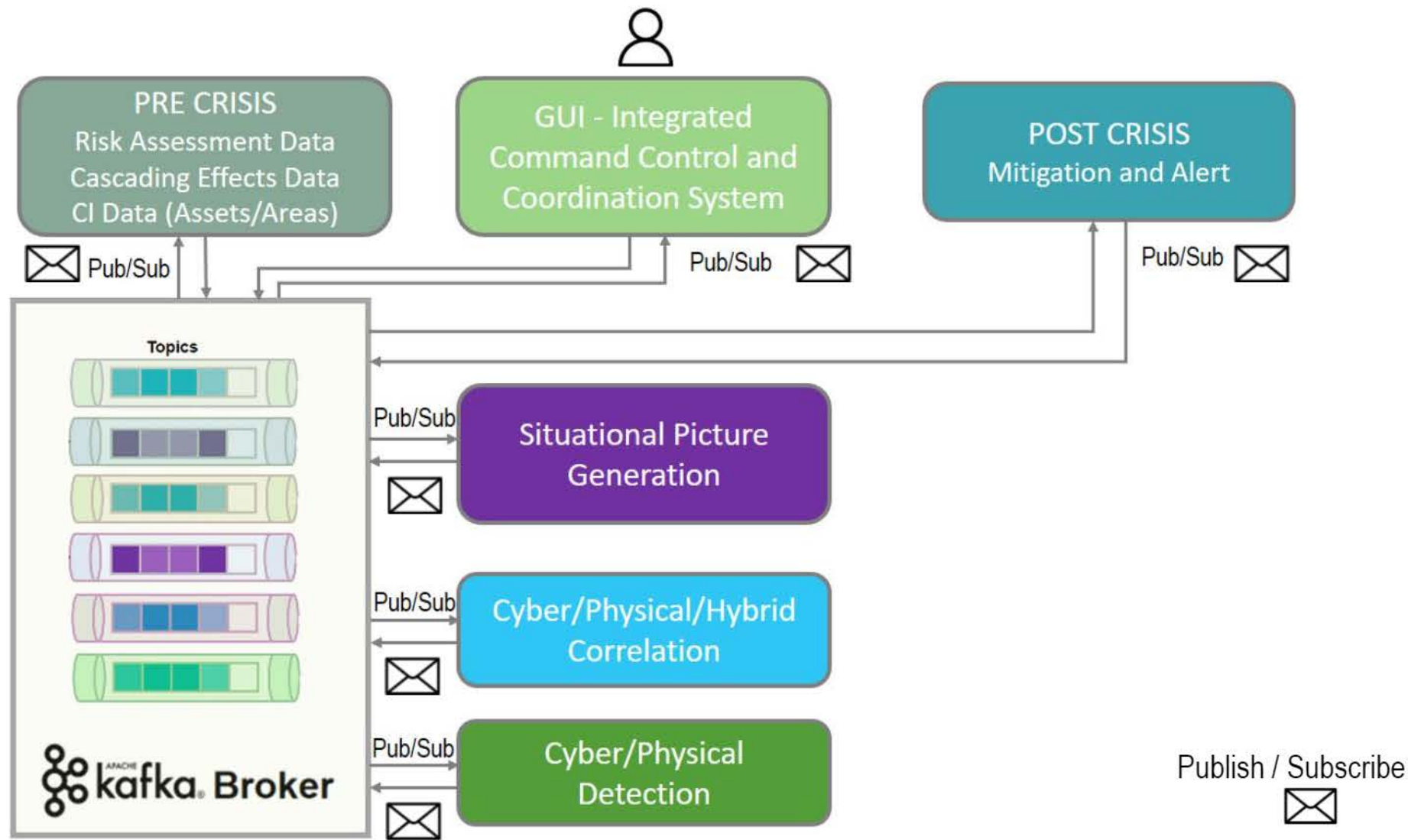
The global architecture of the 7SHIELD platform ensures that all the modules will work together synergistically and effectively to achieve the goal

Define

Identify



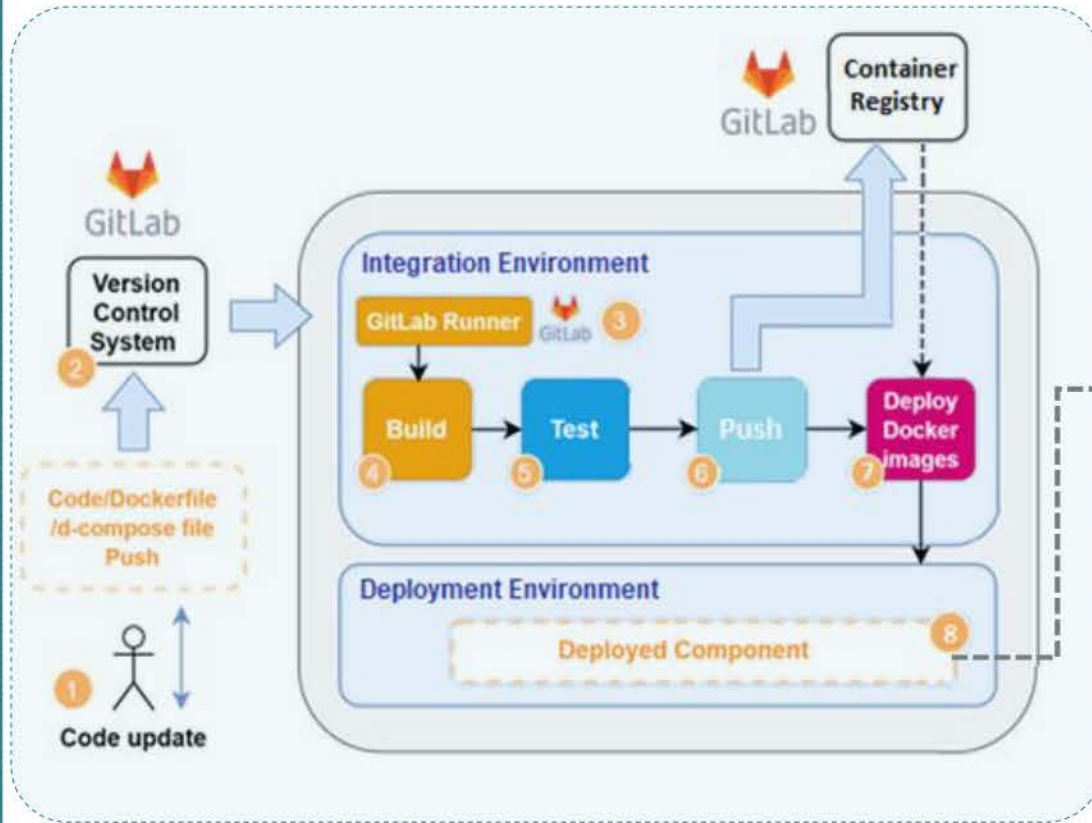
# 7SHIELD platform integration – Event Driven Architecture





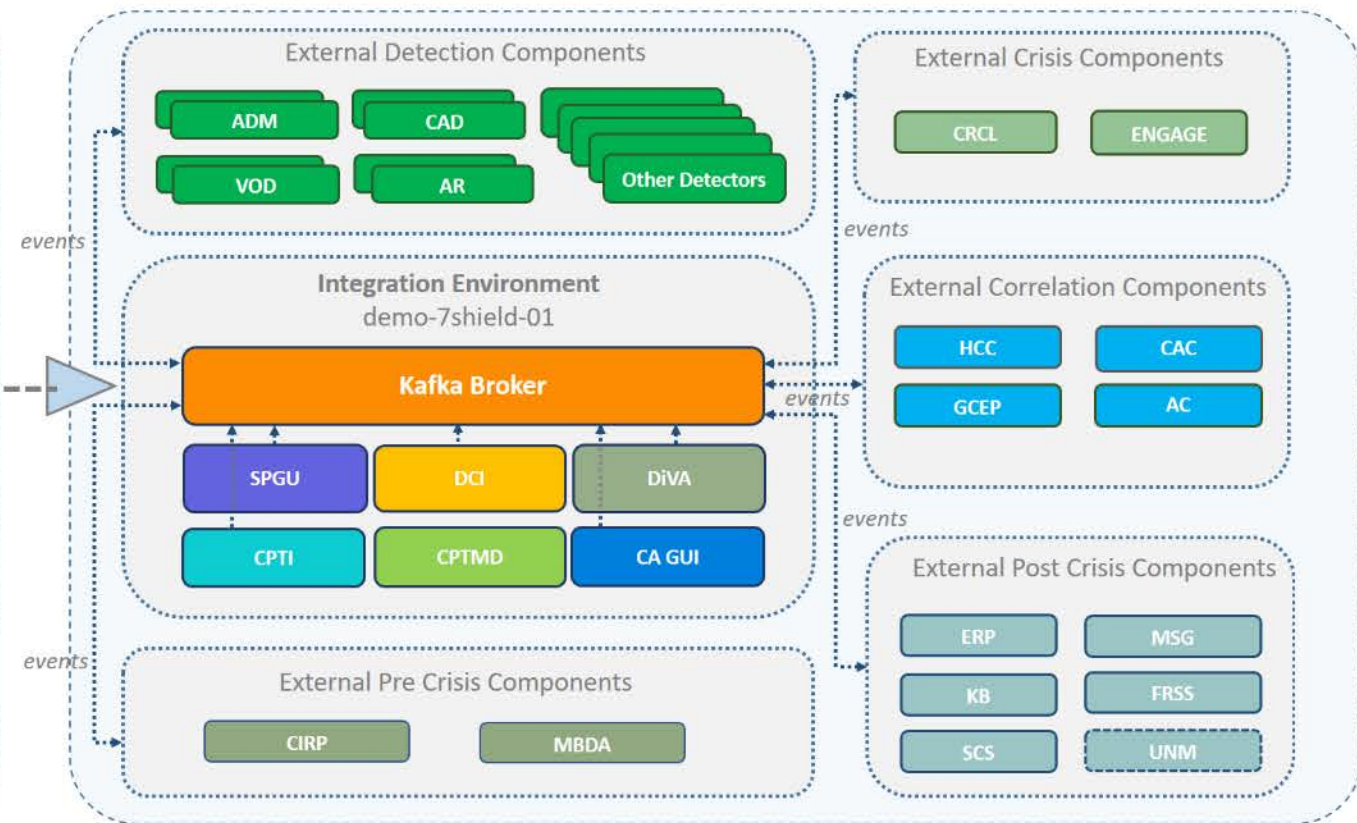
# 7SHIELD platform integration – Integration Environment

## CI/CD



1. A developer pushes code changes
2. The Git Version Control System receives changes
3. The push will automatically Trigger the GitLab CI/CD pipeline
4. Build the application image
5. Run tests against the created image
6. Push the image to a remote registry
7. Deploy a Docker container to a server from the pushed image
8. The application is deployed, live and running in the Deployment Environment

## Distributed Integration Environment



Highly Available

Reliable

**Resulting Infrastructure  
Architecture**

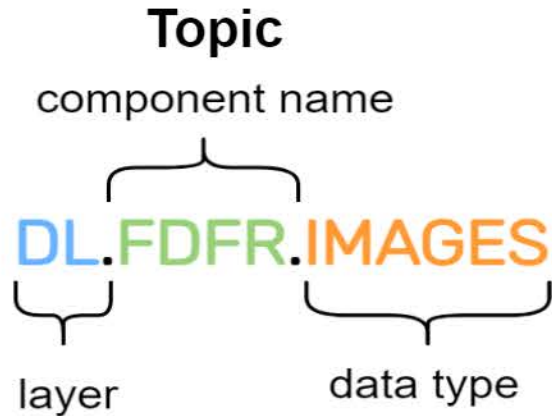
Flexible

Efficient



# 7SHIELD platform integration – Interfaces and criteria for Integration

## Rules for standard data Exchange



## Message

Unique Identifier → **"id": "66c759ae"**,  
Message Version → **"version": "1.0"**,  
Partner Name → **"partner": "ENG"**

## Message Specifications

Component name	Cyber and Physical Threat Intelligence (CPTI)
Topic name	<b>SL.CPTI.OUTPUT</b>
Role [Producer/Consumer]	Producer
Purpose	Send events to 7SHIELD interface
Version	1.0
Scope of interaction	This message is used to send events (alerts) on discovered threats.
Interaction paradigm [P/S   R/R]	P/S
Message Example	<pre>{   "id": "CPTI_UAF_/f0ad63b-22f6-47c8-a5af-0b2ddaac-8bd",   "version": "1.0",   "partner": "Engineering",   "analyzer": [     {       endTime: 1656602741944,       id: 'CPTI_JOBTI_08a95cb2-2166-487e-ab1c',       model: 'ENG',       name: 'TI Core',       notes: '',       startTime: 1656602200803,       version: '1.0'     }   ],   category: [   ] }</pre>





All the 7SHIELD components  
have been integrated and delivered  
in the final version of the platform





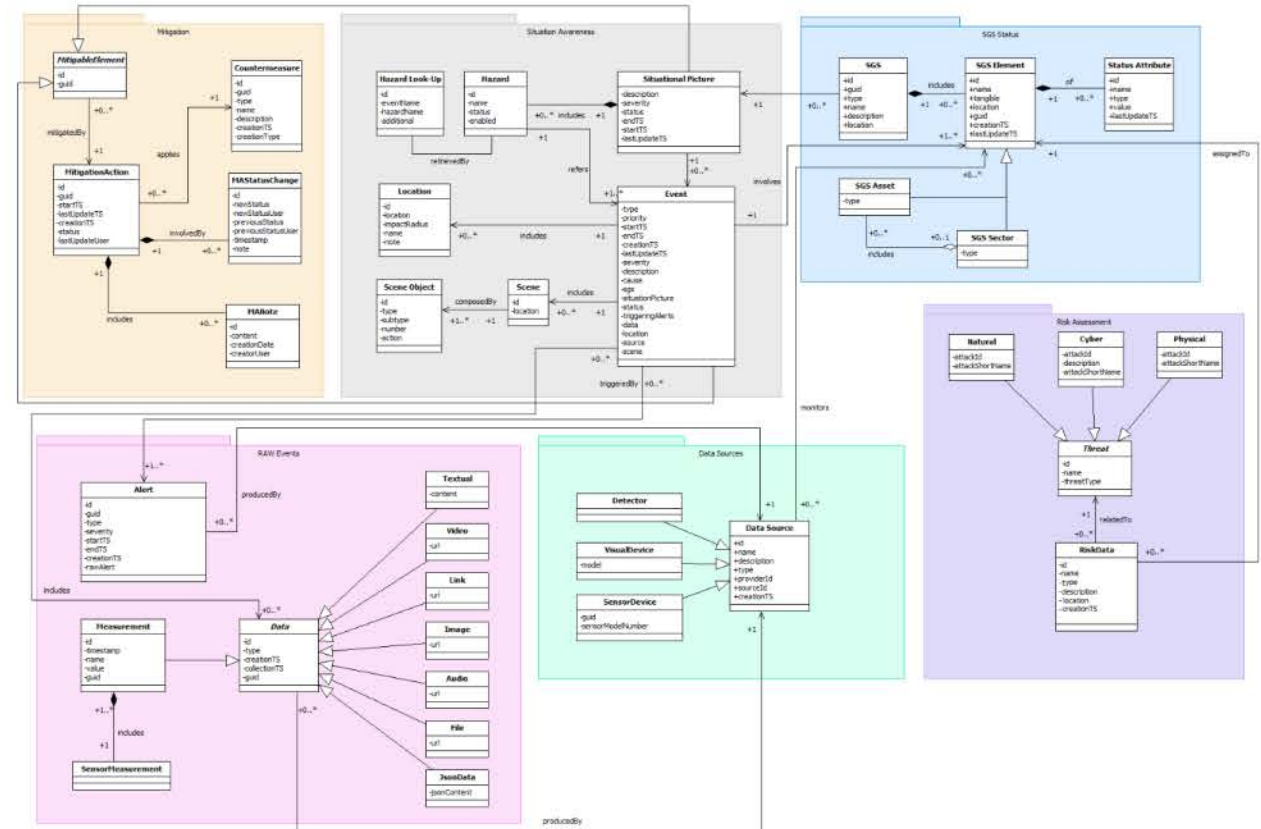
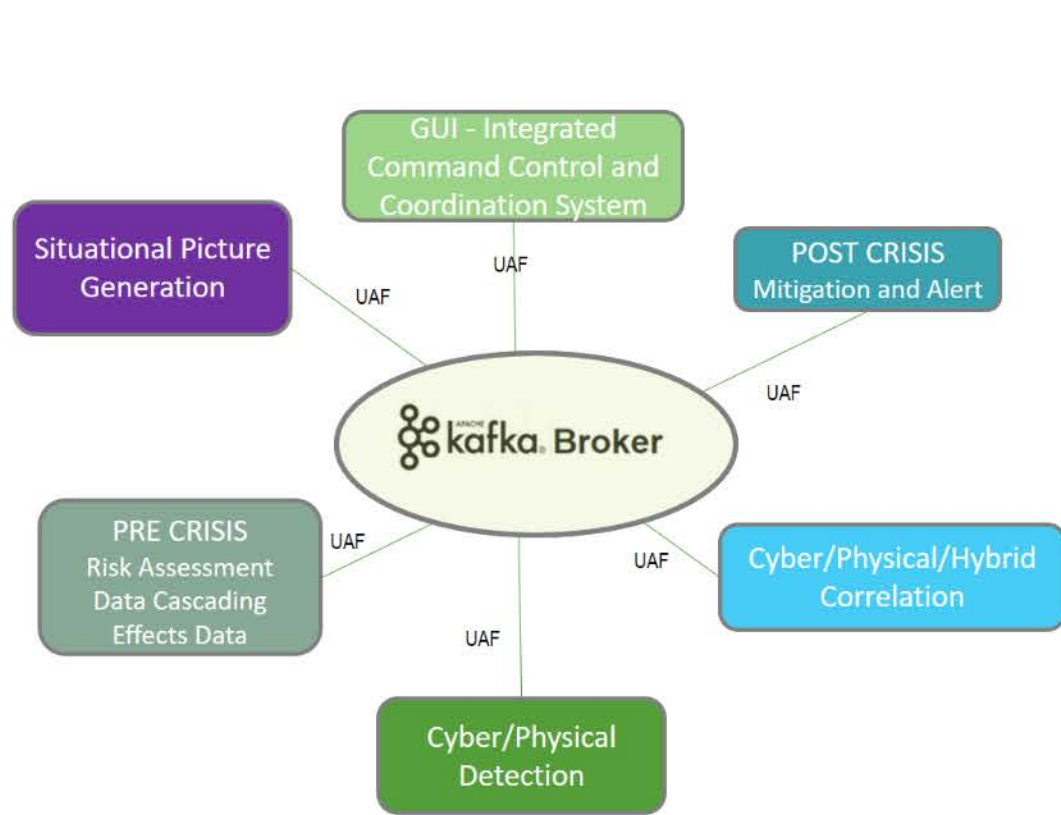
# Data Models for Combined Detection

7SHIELD defines a set of data models enabling

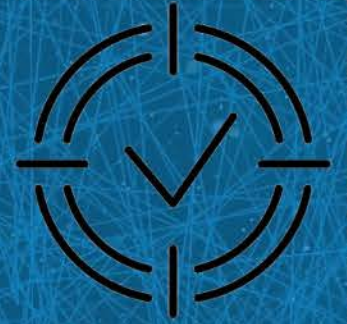
- ✓ Data portability
- ✓ Data Interoperability
- ✓ A Data model for the C-P Situational Awareness



# Unified Alert Format and Situation Awareness Data Model







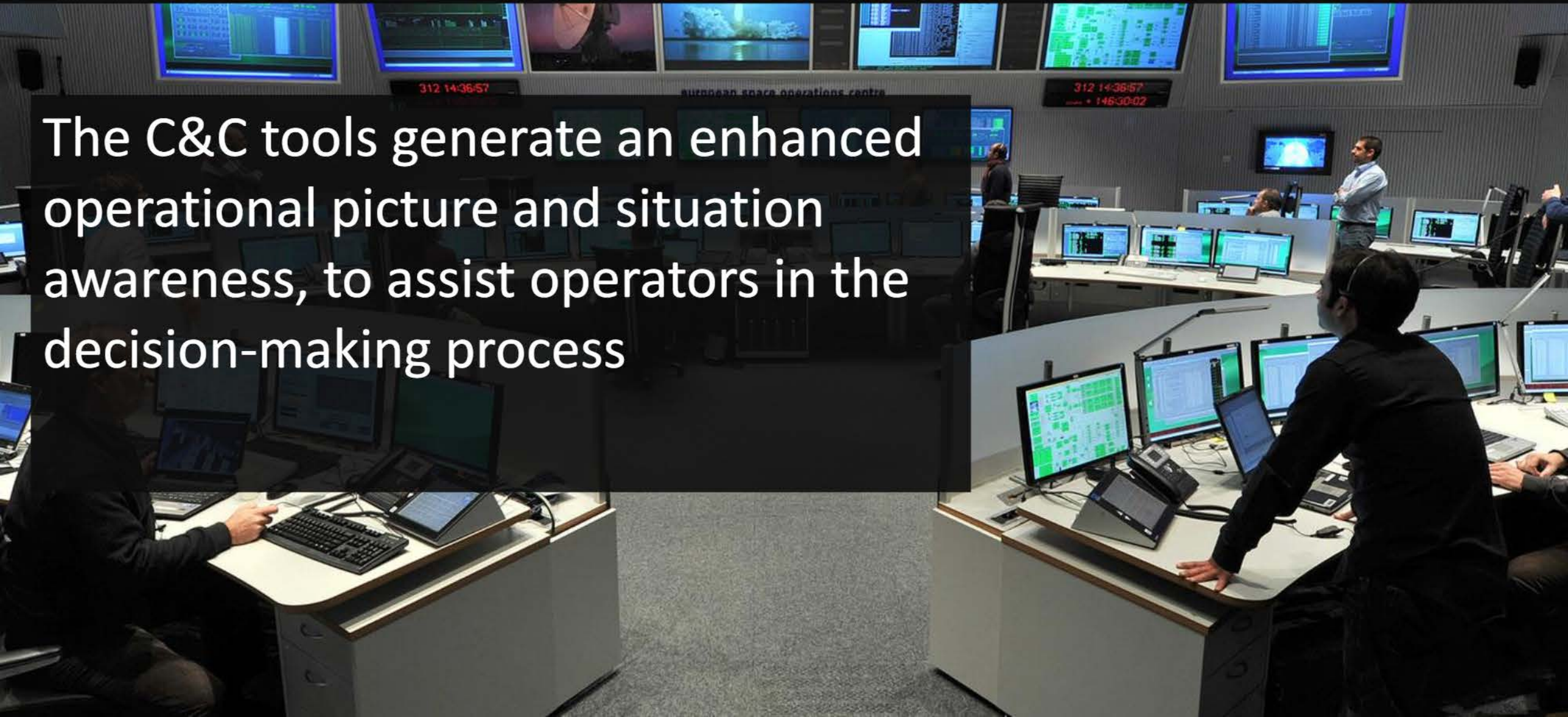
- A semantic layer of interoperability based on the **UAF**
- An enhanced Data Model to optimize the **SPs**





# User Interface-Command and Control Room

The C&C tools generate an enhanced operational picture and situation awareness, to assist operators in the decision-making process

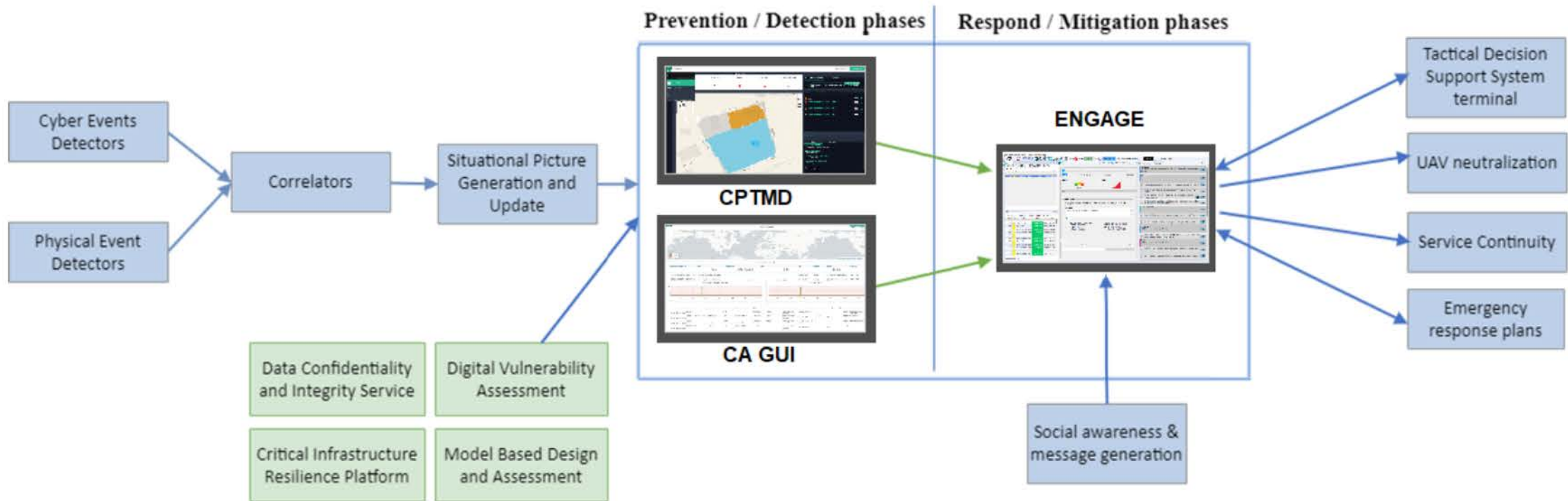




# User Interface - Command and Control Schema

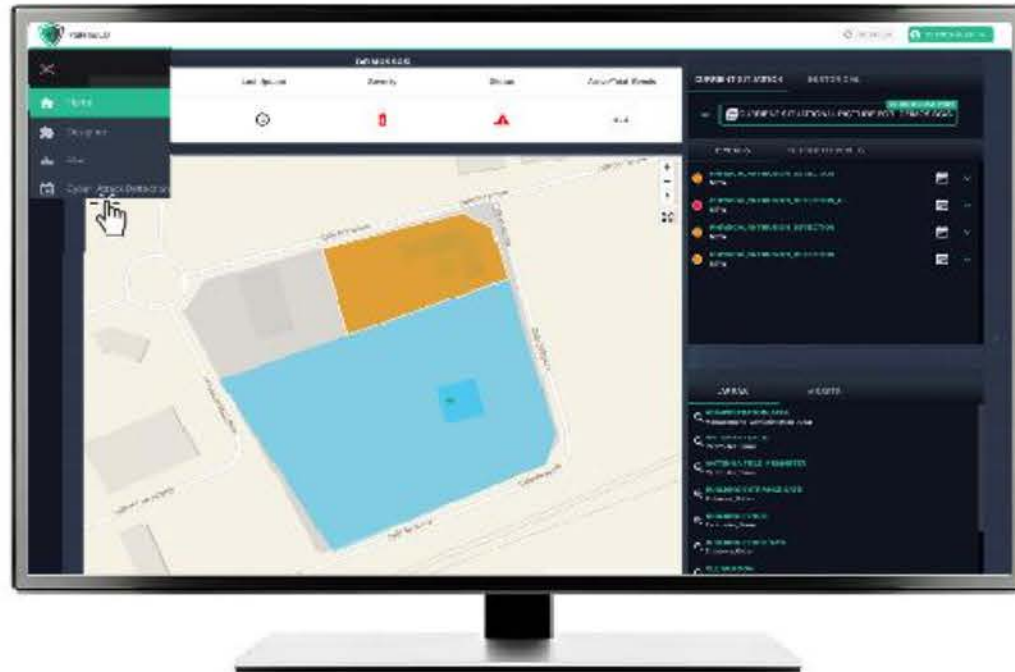


*Operators should be able to analyse single and correlated data*





# Cyber Physical Threat Monitoring and Cyber Attacks Dashboards



**CPTM**

**Cyber-physical Threat Monitoring  
Dashboard**

*Displays the evolution of  
Cyber and Physical threats*

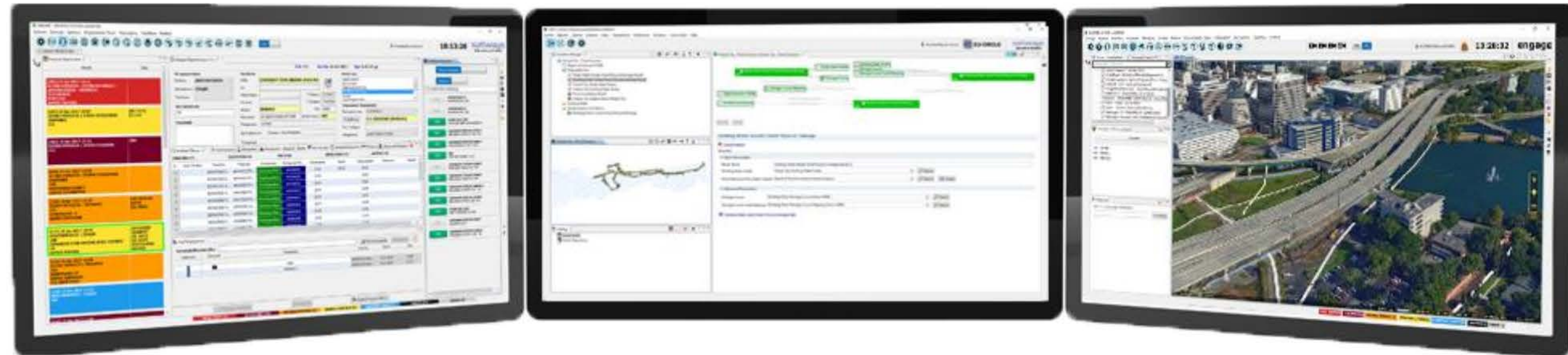


**CA**

**Cyber Attacks  
Dashboard**

*Shows the results of the Cyber-attack  
Detection framework*





## ENGAGE Converged Security Information Management

Engage provides a real-time **Situational Picture** with data from multiple components

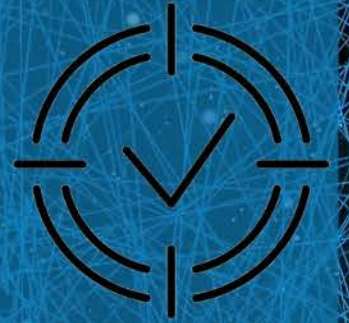
**Events** are listed and prioritized

**Alarms** are mitigated





Information on the updated situation and on threats is immediately available to operators on **CPTM** and **CA** Dashboards



The **ENGAGE** Dashboard allows the management of the situation



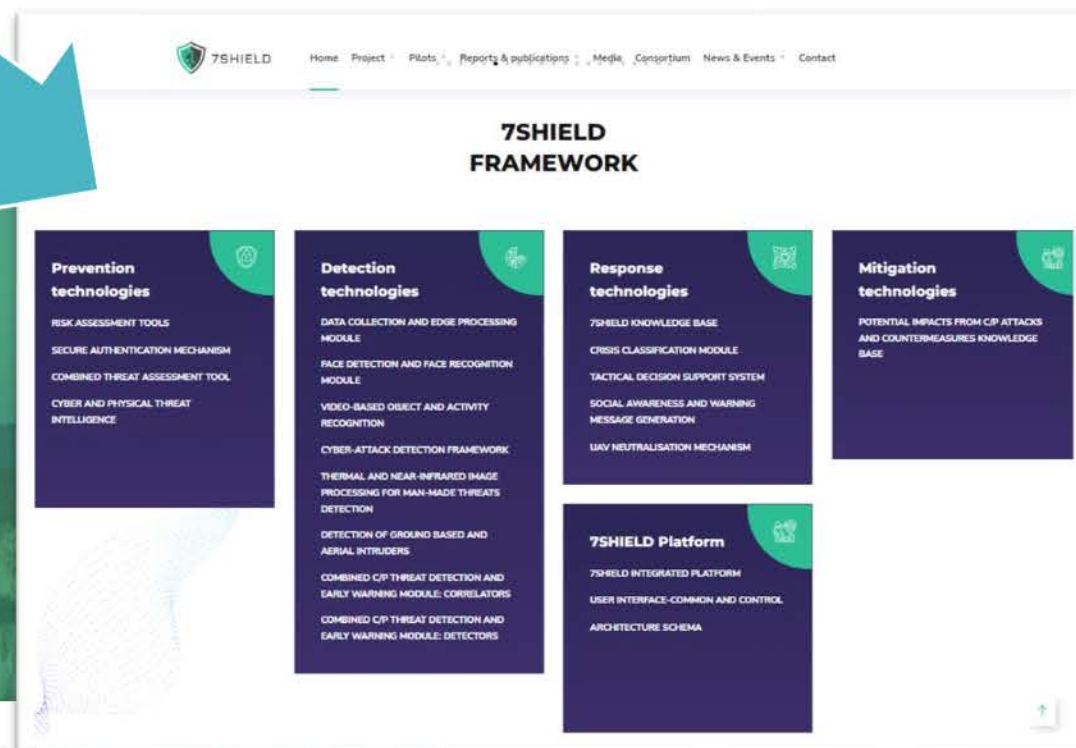
# Further questions?

- Use flipcharts/chat
- Check the walls/KR leaflets on the website

<https://www.7shield.eu/>



7SHIELD



innovation programme under the grant agreement No 883284.



# Lunch Break

The meeting will  
restart at  
**1:50 PM CET**



The poster is titled "7SHIELD Info Day Agenda" and lists the schedule for the event. It includes icons for each session: a group of people for Welcome, a play button for Introduction, a group of people for Stakeholders' experience, a coffee cup for Coffee break, a presentation screen for Demo pilots, a group of people for Innovation activities showcase, a satellite for Physical elements, a shield for 7SHIELD platform adaptability & flexibility, and a handshake for End of meeting. A red dashed box highlights the lunch break and the thematic areas of security session.

7SHIELD Info Day Agenda	
08:30-09:00 Welcome	12:30-13:30 Lunch break
09:00-09:30 #1 – Introduction Context and purpose of the project: why the Ground Segments need to be protected	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.
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.	15:00-15:15 Coffee break
10:30-10:45 Coffee break	15:15-16:15 #6 – Physical elements How to maximize the physical security of existing facilities and buildings with custom solutions
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.	16:15-16:45 #7 – 7SHIELD platform adaptability & flexibility 7SHIELD ability to cope with and adapt to unexpected situations in any Critical Infrastructure
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 attacks. How the integration of state-of-art technologies can improve the security of Ground Segments.	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 844024

**7SHIELD**

Note: the meeting room will be reset up so please leave your personal things near the wardrobe

