Grant number: 883286
Project duration: Sep 2020 – Feb 2023
Project Coordinator: Joe Gorman, SINTEF

Horizon 2020: Secure societies
SU-INFRA02-2019
Security for smart and safe cities, including for public spaces
Project Type: Innovation Action

http://www.impetus-project.eu/

Final Report

Release 1.1 2023-06-15

This document describes of the objectives, results, achievements, and lessons learned from H2020 project IMPETUS.

It provides a public summary intended for a wide audience. Further details are available in project deliverables, accessible via the project website (address above).[1]

Formally, this document constitutes project deliverable: D10.4 "Final (Public) Report"

The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n° 883286.

[1] In a few, limited, cases some text from other project deliverables has been included in this document.

Table of Contents

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

1 Introduction to IMPETUS

1.1 Facts about the project

Project title:	*IMPETUS:* **I**ntelligent **M**anagement of **P**rocesses, **E**thics and **T**echnology for **U**rban **S**afety
Project Type:	Horizon 2020 Innovation Action project
H2020 call:	Secure Societies / SU-INFA02-2019
Duration:	September 2020 – February 2023
Budget:	9.3 M€, EC contribution 7.9M€
Coordinator:	SINTEF, Norway
Consortium:	Research/Univ (5), Industry & SMEs (6), NGOs (3), Municipalities (2) *Full list on final pages of this report*

1.2 Project goals and approach

The goal of IMPETUS is to provide city authorities with new means to **improve the security of public spaces in smart cities**, and so help protect citizens.

To achieve this goal, the project delivers an advanced, technology-based solution that helps operational personnel, based on data gathered from multiple sources, to work closely with each other and with state-of-the art tools to detect threats and make well-informed decisions about how to deal with them.

A distinguishing feature of IMPETUS is that its approach is not purely technological; it provides a solution that operates at the intersection of three areas:

- **Technology**: leverage the power of Internet of Things, Artificial Intelligence and Big Data to provide powerful tools that help operational personnel manage physical and cyber security in smart cities.
- **Ethics**: Balance potentially conflicting needs to collect, transform and share large amounts of data with the imperative of ensuring protection of data privacy and respect for other ethical concerns - all in the context of ensuring benefits to society.
- **Processes**: Define the steps that operational personnel must take, and the assessments they need to make, for effective decision making and coordination - fully aligned with their individual context and the powerful support offered by the technology.

Figure 1: The IMPETUS intersection

1.3 Technology – supported by Practitioners Guides

From a technological point of view, IMPETUS consists of:

1. A set of *individual tools*, each with a specialist purpose. They are grouped as follows:
    - Detect emergencies requiring immediate response.
    - Identify potential/emerging threats.
    - Facilitate management of emergency situations.
    - Protect against cyber threats.
    - Ensure operational efficiency of security staff.
2. A unifying *platform* which allows different security staff to share a common view and interact with tools via a single interface. Legacy tools and future tools can be integrated in the platform.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

The technology is supported by a set of *Practitioners Guides ("PGs")* providing guidelines, documentation, and training materials in the areas of **operations**, **ethical/legal issues** and **cyber security**. They are presented in an online, browsable format that can be easily refined and extended over time. A sound understanding of these areas is needed by organisations/individuals who choose to use IMPETUS (or similar solutions), and the PGs aim to help them obtain that understanding. The PGs are considered as essential "pillars" to support successful adoption and deployment of the technology.

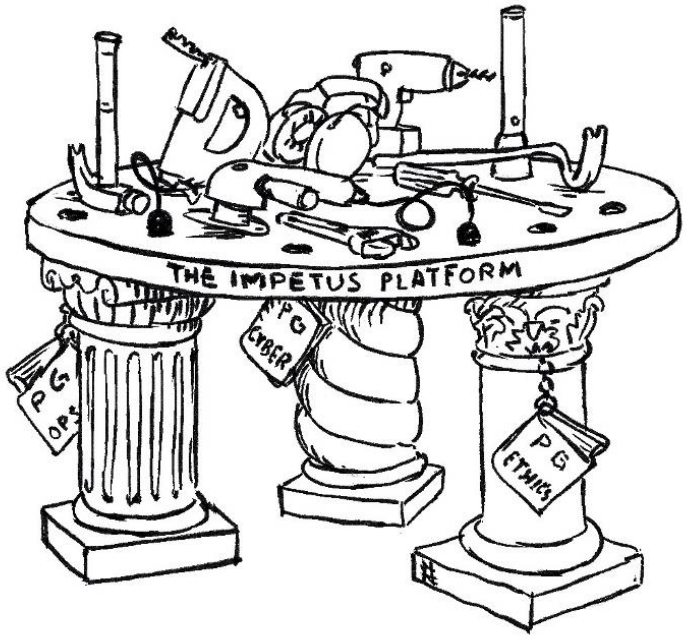


Figure 2 The IMPETUS tools operate on the IMPETUS platform, supported by the essential pillars of the Practitioners Guides (PGs) on Operations, Cyber security and Ethics (Artwork credit: Rafal Hrynkiewicz, Thales, Netherlands)

1.4 Trial Cities – demonstrating viability

The cities of Oslo (Norway) and Padova (Italy) hosted practical trials of the IMPETUS solution during the project lifetime. The trials were used not only for technical in-field testing of the technology but also to evaluate its usability in practical settings by real users.

The trials demonstrated the viability of using advanced technology of the type developed in IMPETUS. The long-term goal (beyond the end of the project) is to use the outcomes of these trials as part of a strategy to encourage much wider uptake - not only geographically but also in terms of other technologies that may emerge in the future.

1.5 Consortium – augmented by wider community (COSSEC)

The project work was carried out by a consortium of 16 partners from 11 different EU Member States and Associated Countries. It brought together 5 research institutions, 6 specialist industrial and SME companies, 3 NGOs and 2 local government authorities (the trial cities).

An essential complement to the consortium itself was COSSEC – the Community of Safe and Secure Cities. This group was established at a small scale at the start of the project but grew to 47 members by the end (16 municipalities, 7 Citizens organisations, 12 University/research institutes, 7 projects and 5 other organisations). COSSEC members interacted with the consortium in a series of webinars, but also in person at practical trials in the two cities, and at the project's final dissemination event. All of this allowed for close dialogue which provided useful feedback that helped set project directions.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

2 Project Results

This chapter contains "1-pager" descriptions of all the main results of IMPETUS, designed to cover the main points about what each result is for, who would use it for what purpose, and what it does. You can obtain more information about specific results via the project website[2].

The results are grouped as follows:

1. The Practitioners Guides[3] (online documentation with advice on ethics, operations and cyber security)
2. Individual tools offering specific functionality in different areas:
    a. Detect emergencies requiring immediate response.
        i. Firearm Detector
        ii. Bacteria Detector
    b. Identify potential/emerging threats.
        i. Urban Anomaly Detector
        ii. Social Media Detection
    c. Facilitate management of emergency situations.
        i. Evacuation Optimiser
    d. Protect against cyber threats.
        i. Cyber Threat Intelligence
        ii. Cyber Threat Detection and Response
    e. Ensure operational efficiency of security staff
        i. Workload Monitoring System
3. The unifying *IMPETUS Platform* through which users can interact with all of the above tools

[2] https://www.impetus-project.eu/

[3] https://impetus-pg.atlassian.net/wiki/spaces/IPG1/overview

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Practitioners Guides

Bringing the lessons learned
from IMPETUS to a wider audience

WHAT PROBLEM DO THE GUIDES ADDRESS?

Advanced technological solutions to collect, analyse and use data in security operations offer great potential to improve safety in cities. But they cannot just be used "straight out of the box": numerous issues related to ethics, data privacy, cyber security and operational practices must be addressed to enable successful deployment and long-term operational impact.

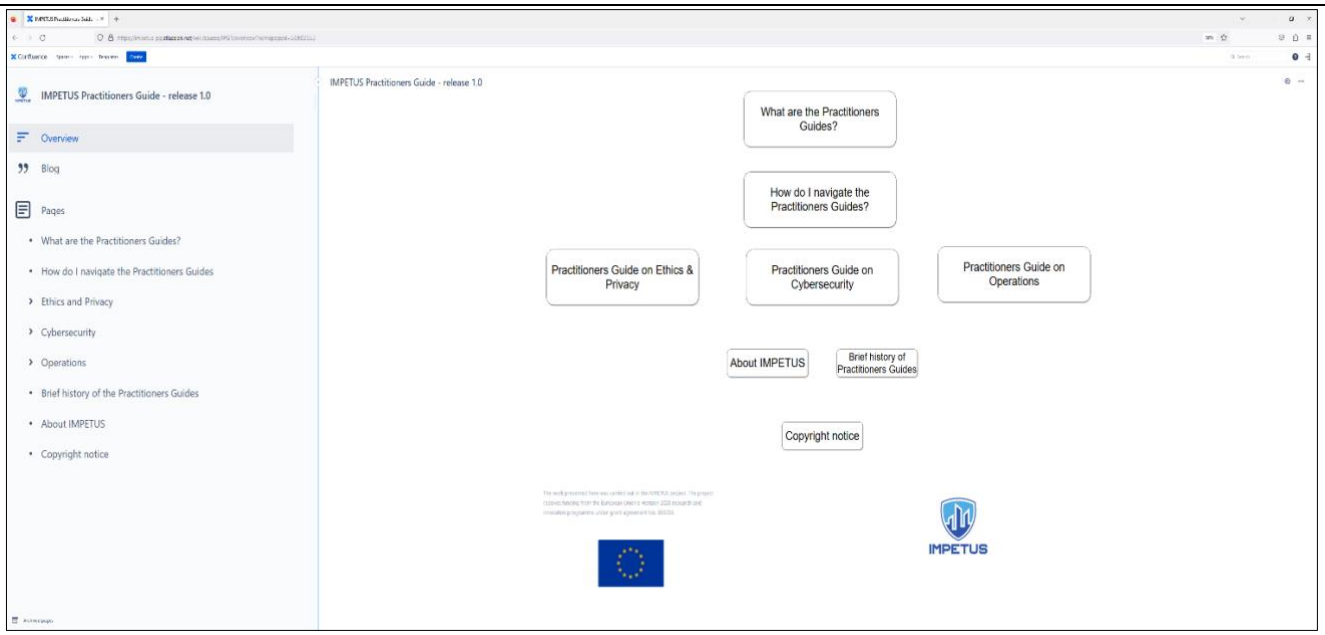
In IMPETUS, we developed approaches to addressing these issues, and learned many valuable lessons along the way. The Practitioners Guides raise awareness and bring lessons learned in IMPETUS to a wider audience. They consist of guidelines, tutorial materials, checklists, reference information and more, covering three core areas:

- Ethics – how to integrate ethical principles and procedures respecting data privacy in operations
- Cyber security – how to guard against, detect and deal with cyber security risks in Smart City contexts
- Operations – how to integrate new technologies into existing working practices to enhance operations

While the guides are based on lessons learned in IMPETUS, they are also applicable in wider contexts related to use of similar technological approaches, and to management and security of Smart environments.

HOW ARE THE GUIDES INTENDED TO BE USED?

- **Who are the readers?** Anyone with any kind of responsibility for security in public spaces, and/or who have specific interests in operational, ethical, legal or cyber security aspects of using advanced technological solutions in security-related operations.
- **How might users benefit?** Readers will understand how to address technical and non-technical challenges in an integrated way so that the advantages of technical solutions can be realised.



HOW DOES IT WORK?

The Practitioners Guides (https://impetus-pg.atlassian.net/wiki/spaces/IPG/overview) are presented in Wiki pages (built using the Confluence framework and tools) with an interactive interface facilitating dynamic exploration of the contents. The aim is to make it easy for readers with different backgrounds and roles to navigate to the modules of interest to them.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Firearm Detector

Continuously monitors surveillance camera feeds and automatically creates an alert if a firearm is detected in a public space

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

Dangerous scenarios and extreme events involving use of weapons, sadly, do occur in our cities. The purpose of this tool is to use surveillance cameras to detect firearms in real-time and improve the physical security of open spaces.

Without this tool:

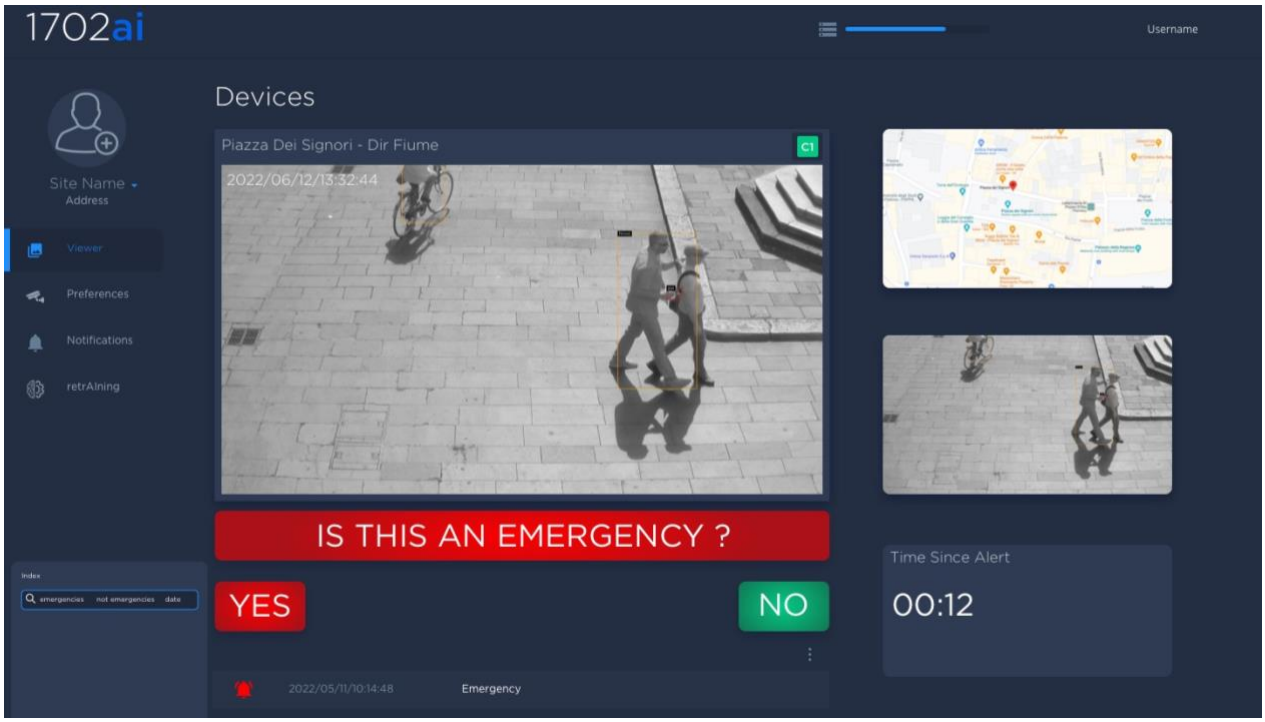
- Law enforcement is hindered due to the lack of detailed situational awareness (delays and uncertainties in reporting, lack of information about exact location)
- Response times can be lengthy – and in situations where every second count, this can lead to loss of life

With this tool:

- Immediate supply of images and location data enables super-fast response times
- The risk of loss of life is significantly reduced
- SOC operations are significantly improved

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: Dispatcher at Security Operations Centres and first responders.
- **What are the critical situations for deployment**: The tool is continuously deployed to monitor and look out for weapons (without any operator intervention). If a weapon is detected, an alert is presented to the security operator who can decide how to respond.



HOW DOES IT WORK?

The instant a weapon enters the surveillance video camera's field of view, an alert is shared with the Security Operations Center. Each alert provides immediate situational awareness. The tool is GDPR, NATO and DHS (Department of Homeland Security) compliant.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Bacteria Detector

Continuously monitors air samples to detect abnormally high concentrations of airborne bacteria

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

The Bacteria Detector continuously monitors bacterial concentration in the air to help protect citizens from biological hazards. It communicates with the IMPETUS platform to raise alerts with the authorities.
Without the tool:

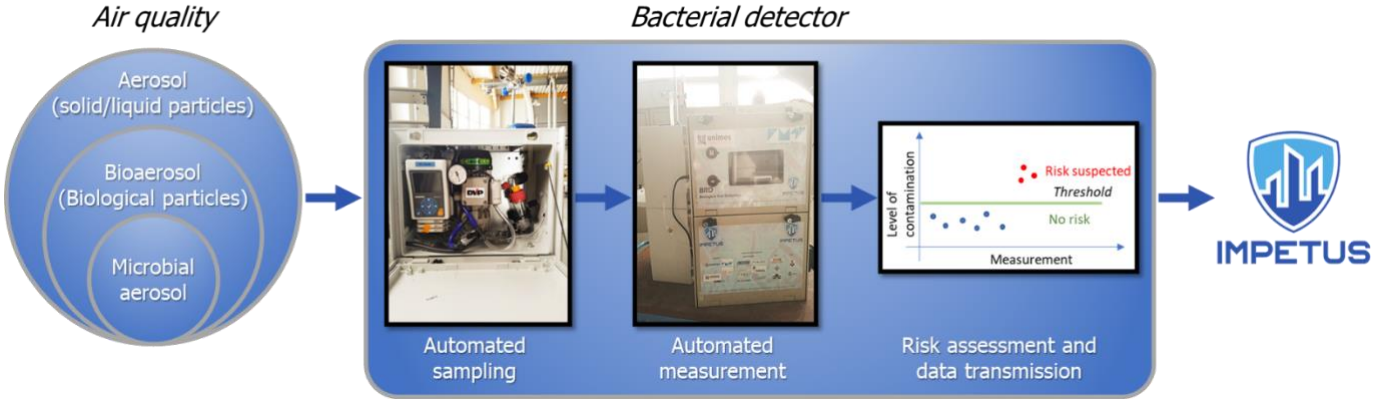
- One person can infect 1–10 other people, depending on the pathogen
- Physicians need to take samples from patients to find a suitable treatment, which prolongs treatment
- Hospital staff are not protected, and an epidemic can be declared the day after the disease appears

With the tool:

- Only those present at the point of infection are contaminated
- Samples are taken in the room and from patients (with a result in <4 hours)
- Physicians readily adapt their procedure and treatment plan, thus saving time
- Hospital staff are protected, and the risk of spreading is limited

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: Trained technicians operate the equipment. Security centre operators and stakeholders in hospitals, government officials, senior level management, etc. receive early notification of possible contamination threats and infectious bacterial outbreaks through online monitoring.
- **What are the critical situations for deployment**: Continuous: the main purpose of the tools is to provide constant situational awareness and raise alerts when needed.



HOW DOES IT WORK?

This tool combines an air biocollector (developed by IMT Alès / University of Nîmes) and a bacterial concentration measurement device. Firstly, air is sampled using an impinger and any bacteria trapped on the device are resuspended in water. Secondly, the water is analysed to measure bacteria in the air. Finally, the data is sent to the IMPETUS platform and an alert is triggered if the measurement exceeds a defined threshold.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Urban Anomaly Detector

Continuously monitors data gathered from multiple city sensors and detects cases deviating from the norm - indicating possible cause for concern

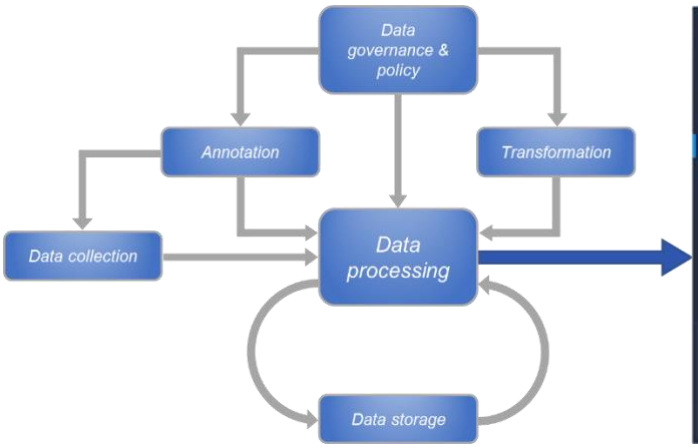
WHAT PROBLEM DOES THE TOOL HELP SOLVE?

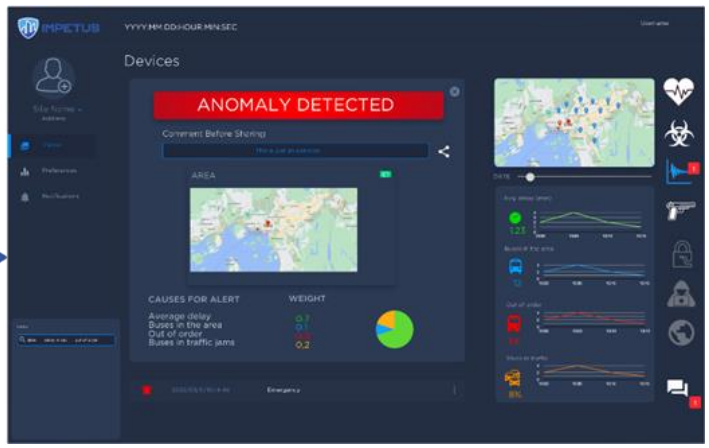
Smart cities continuously gather data from multiple sensors throughout the city. While variations in the data can be a sign of possible problems, the volumes of data are typically so huge that it is not feasible to monitor manually, or easily detect anomalies.
The tool uses AI (Artificial Intelligence) techniques to gather data from multiple sources over long time periods to recognise patterns and recognise what is "normal" at different times and places. It then uses that knowledge to detect anomalies when they occur, even if they have not been observed before. The tool can categorize anomalies and let a human operator evaluate whether they represent a real danger.

- Without the tool: abnormal events or situations can go unnoticed because humans are unable to process the amount of data needed to identify a threat when it occurs, which can lead to chaos and possibly disaster.
- With the tool: any unusual developments are quickly and automatically identified, and steps can then be taken to assess the situation and, maybe, mitigate a disaster.

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: Security, transport and operational personnel monitoring impending physical threats, traffic flow and/or security infringements before and after any abnormal event; other stakeholders such as city managers, government officials, senior level official, etc.
- **What are the critical situations for deployment**: Continuous. The tool aims to provide constant situational awareness – anomalies can arise at any time.





HOW DOES IT WORK?

Large quantities of data are constantly collected from several sources, e.g., CCTV, sensors, municipal properties (details will vary from city to city). These data are processed using policy awareness, analytics and visualisation. If anomalies are detected, a visualisation – showing what is "unusual" – is sent as an alert to the IMPETUS platform, for the attention of emergency operators.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Social Media Detection

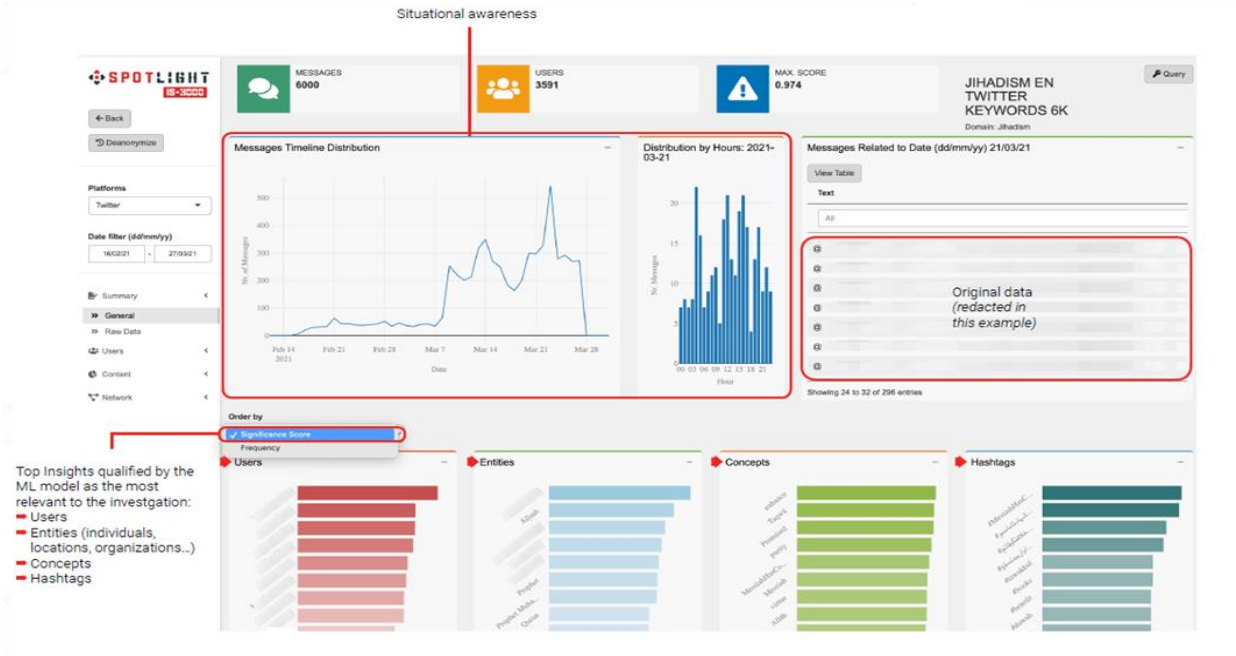
Scans large volumes of text on social media and other public online sites, looking for topics/keywords that might indicate potential trouble or threats

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

The huge amounts of data on social media++ can contain vital information that is relevant for people responsible for public safety – but this information very likely goes unnoticed because it is not humanly possible for people to monitor and analyse the huge volumes. Warnings of possible issues go unnoticed. The purpose of the tool is to increase efficiency and capacity when searching for accurate and relevant insights in the ocean of data published on the open web. As the software expedites data analyses, the user can run multiple search projects, thus expanding and/or fine-tuning their search to obtain more relevant outputs.

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: Intelligence analysts, tasked to give security centre operators early notice of possible dangerous situations/threats or monitoring the aftermath online, which can be of interest to other stakeholders such as government officials, senior level management, etc.
- **What are the critical situations for deployment**: A 3-step process:
    1. Create a project of interest
    2. Acquire and analyse data
    3. Use the dashboard to send alerts when anomalies are detected



HOW DOES IT WORK?

The analyst first creates a project of the topic of their interest using search criteria, e.g. keywords. The tool retrieves massive volumes of data from social media platforms, websites, forums, etc. based on the search criteria. The tool analyses the data, removing unrelated content, and presents the most relevant insights/information for each project. The user receives a notification through the IMPETUS platform that the results have generated. The analyst can then filter and fine-tune the search criteria and results to get more specific and more relevant information. This tool will aid the end user in identifying any hidden threats, or notify the user if unrest is brewing.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Evacuation Optimiser

Provides instant advice to emergency staff on how to effectively manage an evacuation, based on simulations of different evacuation scenarios

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

The main purpose of the tool is to pre-optimise and support the management of controlled crowd movement in public spaces in complex events, to prevent any injury and/or loss of life, e.g., in an emergency evacuation.
Without the tool:

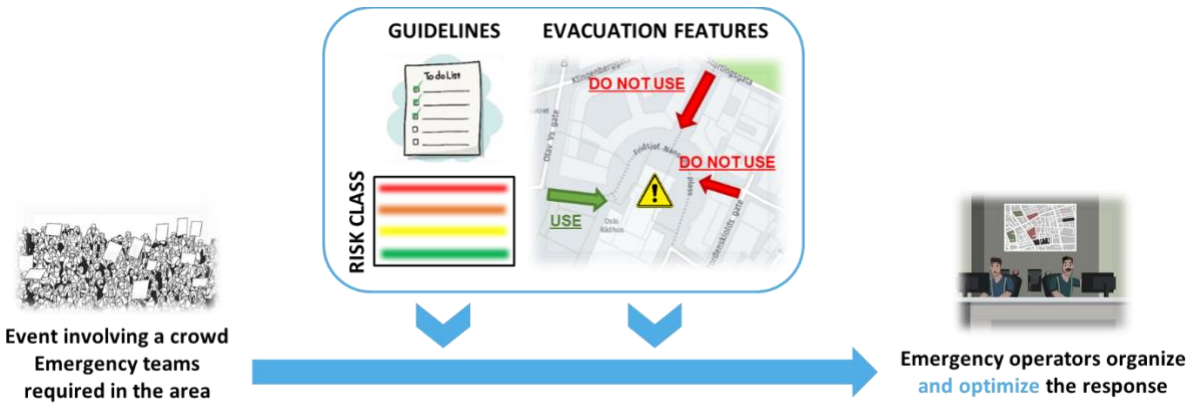
- The adequacy of number and size of exit routes is unidentified
- Specific gateways for emergency services are not known
- The total evacuation time and risk associated with evacuation remain unknown

With the tool:

- The number and direction of exit routes for the size of the crowd is evaluated
- Gateways for emergency services are identified
- An accurate calculation of total evacuation time and risk is presented to emergency operators via the IMPETUS platform
- Successful evacuation procedures

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: First responders and security centre operators who are tasked with early notification of possible dangerous situations/threats, or online, real-time monitoring of the event/emergency; other stakeholders such as government officials, senior level management, city managers, etc.
- **What are the critical situations for deployment**: The tool facilitates coordination between different agencies, staff in control rooms and staff on location, and members of the public in preparation of and during a critical event. It can help dispatch required resources as efficiently as possible. The tool also facilitates planning of and execution of evacuations by mapping the quickest, most direct route for crowd control and movement.



HOW DOES IT WORK?

- **Preparation for an emergency**: Using data from people-counting sensors, the tool pre-simulates evacuation scenarios from a public space under different circumstances and provides general operative guidelines for managing the exit of a crowd in the different scenarios.
- **During an emergency**: Based on data from earlier simulations, the size of the crowd, the number of entry/exit point and the capacity of the evacuation routes, the tool estimates the time needed to evacuate the crowd, and estimates the risk involved. Guidelines on optimal entry and evacuation routes are presented to emergency personnel and security operators via the IMPETUS platform.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Cyber Threat Intelligence

Detects, classifies and helps mitigate cyber space threats to an organisation's IT assets

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

The purpose of the tool is to continuously expose the earliest indication of cyber risks to an organisation's network from deep and dark web fora and markets, as well as private messaging groups.
Without the tool, analysts will have to cope with a lot of manual work, regarding:

- Collecting domain, IP and third-party data
- Indexing, tagging and metadata analysis of collected data
- Extracting relevant data and restructuring and packaging for data storage in a database maintained by the tool provider (Cybersixgill)

With the tool, you are able to:

- Receive and use a queue of asset-based alerts
- Conduct offline and discreet investigation of ongoing threats and events in cyber space
- Receive contextual information of – and mitigate – the threats to the organisation (who, where, what)

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: IT specialists tasked with giving Security Operations Center operators and other stakeholders (government officials, senior level management, etc.) early notice of possible threats posed to the organisation's assets.
- **What are the critical situations for deployment**: Regular: scans would typically be performed daily. The tool provides comprehensive insights into the nature and source of cyber threats, and as these can emerge rapidly it essential to keep up to date.

HOW DOES IT WORK?

There are 3 main steps:

1. **Data collection** – Finding all relevant sources, sign-in closed access forums and groups, and inquire the data (by crawling).
2. **Data processing and analysis** – The tool runs several processes on every newly collected item: indexing, enrichment, tagging, entity extraction, metadata, restructuring and saving the data into a database.
3. **Data lake query** – Automated and manual processes are running on our extensive database of cyber incidents and threat actors' activity.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Cyber Threat Detection and Response

Detects cyber vulnerabilities in IT Systems: raises alerts and suggests countermeasures if they arise

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

Information systems typically have so many vulnerabilities that it is not feasible to continuously monitor or manually manage all of them. Moreover, there are complex dependencies between vulnerabilities. For example: some vulnerabilities only become critical when some other vulnerability has been exploited (i.e., there has been a successful attack). This tool:

- Identifies exploited threats and potentially exploited vulnerabilities
- Prioritises actions to tackle the exploited threats and any exploitable vulnerabilities based on criticality of the situation

Without the tool:

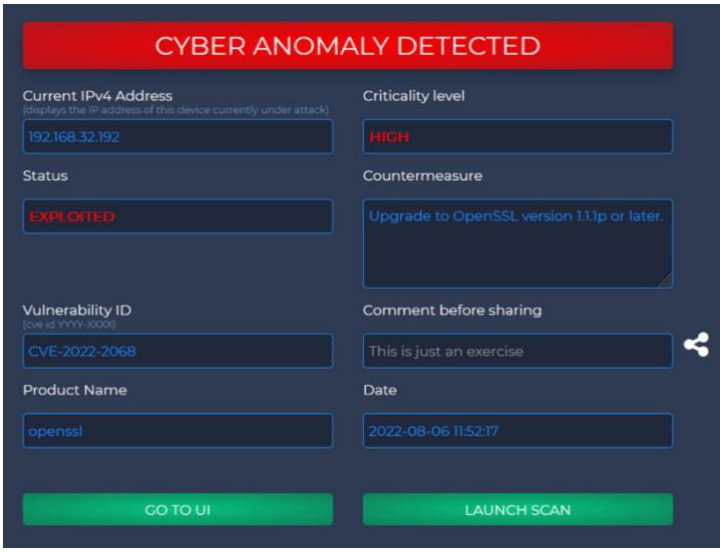
- Users' manual analyses of the system identify only a fraction of the vulnerabilities inherent within the system
- Users are not aware of how inter-linked vulnerabilities could expose the system
- Users are not aware when a vulnerability has been exploited

With the tool:

- Users can scan complex systems to identify all vulnerabilities and their relationships
- Users can monitor systems in real-time and receive an alert on the IMPETUS platform when a vulnerability has been exploited
- Countermeasures can be prioritised based on the criticality of the threat

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: (A) IT specialists responsible for protecting IT infrastructure against possible cyber-attacks (through analysis, monitoring and mitigation); (B) System operators and Security Centre operators who need notification of imminent threats/problematic situations.
- **What are the critical situations for deployment**: Regular: scans and analyses would be performed periodically. The tool is designed to provide up to date situational awareness.



HOW DOES IT WORK?

The tool monitors network traffic data and correlates it with vulnerabilities discovered from a network scan. When an anomaly threatening a vulnerability on the system is detected, remedial actions are prioritised based on the severity of the threat. A cyber security alert is generated, which is sent to the IMPETUS platform. Users can then take the prescribed action to mitigate the threat. For example, when a user tries to remotely access a machine several times, the tool will generate an alert to the IMPETUS platform suggesting the necessary countermeasures.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Workload Monitoring System

Measures mental workload and stress of emergency operators using a brain-computer interface, raises alerts if anomalies arise

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

A SOC (Security Operations Centre) can be a highly stressful working environment, and staff may react slowly or even make mistakes if stress goes unnoticed. The opposite situation – too little to do – can lead to boredom and inattentiveness.
This tool minimizes potential human error and improves human–machine teaming performance by monitoring the physical, emotional and mental workload status of operators while they perform their duties. It provides an early notification of an individual and/or a team's workload capability and ability to cope with stressors during emergencies.
Without the tool:

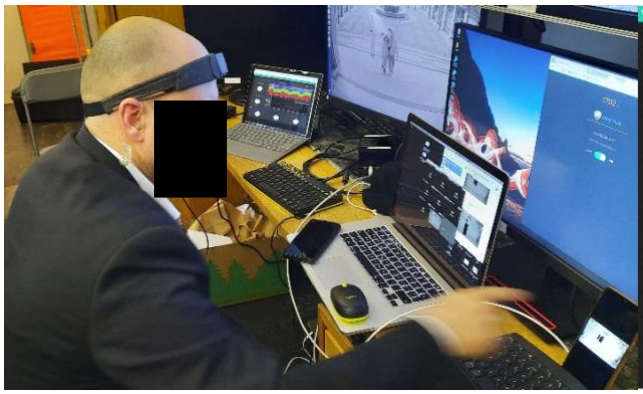
- Workload perception is implicit, subjective and sporadic

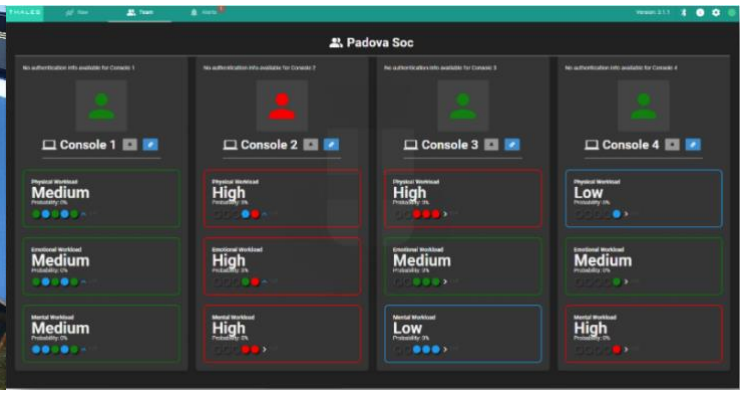
With the tool:

- Workload assessment is explicit, objective and continuous

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: SOC operators and supervisors, IT specialists, behavioural scientists, stress analysts.
- **What are the critical situations for deployment**: The tool and its sensors are unobtrusive and can be deployed continuously while operators are working, including during emergencies.





HOW DOES IT WORK?

Each operator wears an unobtrusive wearable headband which detects bio-signals (pulse, brain waves) and transmits these to the tool. Operator workload is predicted based on personalised, pre-trained (machine learnt) models. The tool can be used at individual and team levels. The supervisor is alerted when an anomaly is detected.
The graphical user-interface provides the supervisor with an overview of:

- Workload status of each team member, including trends over-time
- Alerts related to:
  - sensor data availability (e.g., in case of sensor failure)
  - workload (too high/too low) for any of the operators

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

The IMPETUS Platform

Integrates multiple tools in a unified interface

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

People involved in security operations often need to deal with multiple tools at the same time. At a given moment they may be interacting directly with just one specific tool – but they need to be made immediately aware of critical situations that other tools may have detected. If tools interact with users via separate interfaces, it can be very difficult for staff to work effectively, especially in stressful situations. Also: different users may have different perceptions of the overall situation depending on which tools they happen to be using.

The IMPETUS platform provides a way to combine multiple tools in a unified interface, so that users who need to interact with multiple tools can do so in one place. It shows the status of all the tools (example: an urgent alert has been raised) and allows an operator to interact with a specific tool to get more information. It supports common situational awareness as different operators have the same overall view. It also offers possibilities to produce customised interfaces fine-tuned to the needs of different users (depending on their role, some users might be primarily interested in different subsets of the tools available).

The platform already supports integration with the tools developed in the IMPETUS project, but it is designed in an open way so that other tools (ones already in use by an organisation, or new ones they might acquire in future) can also be integrated.

HOW IS IT DEPLOYED IN IMPETUS?

- **Who are the users**: Emergency and security centre operators and their supervisors; IT analysts and technicians; other staff responsible for monitoring and dealing with urban security.
- **What are the critical situations for deployment:** Continuous: Security is a 24/7 operation.

HOW DOES IT WORK?

The platform provides a central dashboard integrating tools to allow monitoring of potential threat events as they arise. There is a main dashboard showing the overall status of all tools, and tool-specific dashboards to allow more detailed interaction with specific tools.
Alerts are shown with different levels of priority, and indications of whether they have been acknowledged and/or resolved. Where feasible, data is presented graphically for easy visualization, and a map is provided to show where the event occurred. Comments can be associated with alerts and shared with other users.
The platform was implemented using the Snap4City platform: http://www.snap4city.org/

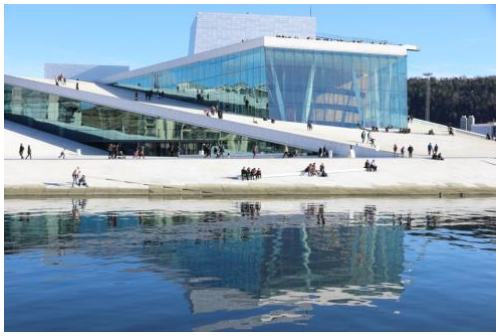
This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

3 Practical trials in two cites: Oslo and Padova

Further details about the practical trials can be found in project deliverable D7.3 "Report on the use of the technical platform in pilots".

3.1 Two types of trials: "Acceptance Pilot" and "Live Exercise"

Testing of technology in practical settings was a central part of the project. The main events that took place were:

	Oslo	**Padova**
		
Acceptance Pilot	3rd – 5th November 2021	1st – 3rd December 2021
Live Exercise	18th August 2022	5th-6th October 2022

In addition to these main events, there were several intermediate/bridge meetings where lessons learned from earlier events were used to refine plans for forthcoming events.

The goals of the Acceptance Pilot events were to:

- Define scenarios that would provide opportunities for all IMPETUS results to be tested.
- Help both IT staff and end-users to understand the functionality offered by the tools and platform.
- Perform any customisation needed in tools for deployment at the trial site.
- Carry out technical testing of the technology.
- Provide an initial opportunity for some end-users to try some of the tools and give feedback.
- Use observers from the project team to witness practical usage of tools, interview end-users and carefully document findings and feedback.

In addition to project participants, the Acceptance Pilots were attended by some potential end-users from the cities. A small number of COSSEC member attended the Padova Acceptance Pilot. It was not necessary to involve "volunteers" for the scenarios.

The Live Exercises were larger scale and more ambitious in scope than the Acceptance Pilots:

- Scenarios were extended and refined.
- Many more people external to the project team were directly involved in the exercise itself:
  - Representatives from security services, including different departments/groups.
  - External "volunteers" to play roles as members of the public.
- Involvement of multiple members of COSSEC (see section 1.5). The COSSEC members observed the exercises, and in de-brief discussion after the exercise itself engaged in lively discussion about technical, practical, and ethical issues related to what had been observed.
- As part of each event, an informal Exhibition was arranged with a stand for each project result. This allowed external guests (security staff, decision makers, local politicians and COSSEC members) to learn more in detail about individual results – and provide their views on these.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

The focus of the Live Exercises was on *validation* (i.e., assessing whether the IMPETUS solution would address real needs in a practical setting) rather than on testing whether the technology worked at the technical level. The key questions to be asked were whether use of IMPETUS technology:

- Improves situational awareness.
- Allows decisions to be taken more quickly.
- Reduces the number of errors.
- Improves coordination (meaning a smoother cooperation with different agencies, sectors, first relievers, patrols on the field, etc.).
- Provides more accurate information.
- Provides additional information or alerts that are not currently possible.

As for the Acceptance Pilots, observers carefully documented what occurred. In addition, questionnaires were used to gather detailed feedback.

3.2 The Oslo Live Exercise

The Live Exercise in Oslo took place in and around Oslo City Hall.

Figure 3: Oslo City Hall –main location of the Live Exercise

The Live Exercise that took place in Oslo was a large event involving multiple actors at multiple locations, and a scenario consisting of a complex sequence of events. Only part of the overall exercise that took place made direct use of IMPETUS technology. The overall exercise continued for several hours after the IMPETUS technology part, involving evacuation by public transport, establishment of a next-of-kin centre, Police SOC handling, and involvement of the Fire and Rescue department). Doing things this way provided a better frame of reference to assess how IMPETUS could affect cascading consequences of the scenario, rather than to close the exercise after the IMPETUS part of the scenario was over.

Key points about the Oslo exercise:

- Based on a scenario including:
    - Demonstrators outside the city hall.
    - A gunman in the crowd, with a visible weapon.
    - Bacterial attack.
    - Evacuation of the building.
    - Cyber-attack.
- The events in the scenario happened in rapid succession, putting great pressure on the operators in the Security Operations Centre (SOC).
- All events in the scenario were directly relevant to at least one of the IMPETUS tools.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

- In addition, the Live Exercise included integration with TRIO, a tool already in use by Oslo for communication with staff in the field.

Figure 4: Inside the SOC

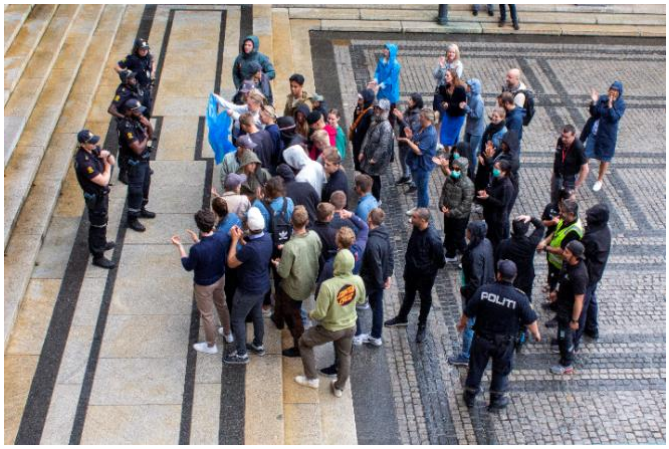


Figure 5: Demonstrators in front of city hall

Figure 6: Fire and rescue - bacterial decontamination

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

3.3 The Padova Live Exercise

The "action" part of the Padova exercise took place in Piazza dei Signori in the heart of the city.

Figure 7: Piazza dei Signori, Padova

In addition, there were key actors at multiple other locations in the city:

1. *Office "Polizia Giudiziaria", Via Liberi:* hosted the test session related to intelligence activities.
2. *IT Department – HQ, via Sarpi:* intelligence analysts and the SOC operators, also the IT specialist experts used the cyber security tools directly in their own workstations.
3. *SOC and HQ, via Gozzi:* the SOC operators, directly using their daily workstations, took their countermeasures against what was occurring in the square getting inputs, alerts and additional information from the IMPETUS platform and tools.
4. *Office "Polizia di Prossimità", Prato della Valle:* Consortium members and external guests gathered here and could see the same screen images as the SOC operators. This location was also used for interactive sessions with the audience, and for the exhibition.

Key points about the Padova scenario:

- Both National Police and local Carabinieri (military branch police force) were involved, located at their own SOCs.
- Based on a scenario including:
    - Problems with high workload for SOC operators.
    - Abnormal traffic flows and crowd gathering in the square at an unexpected time.
    - Gunman observed approaching the square.
    - Evacuation following bacterial alert leading to further confusion in the square.
- As in Oslo, all events in the scenario were directly relevant to at least one of the IMEPTUS tools.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

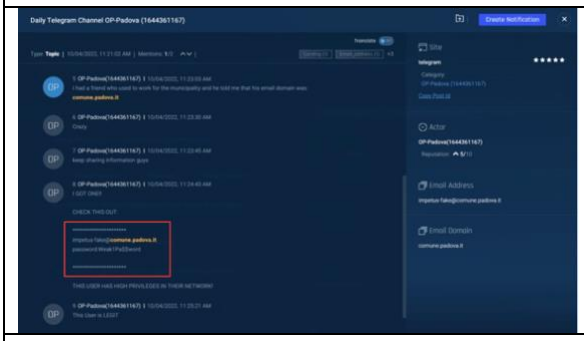
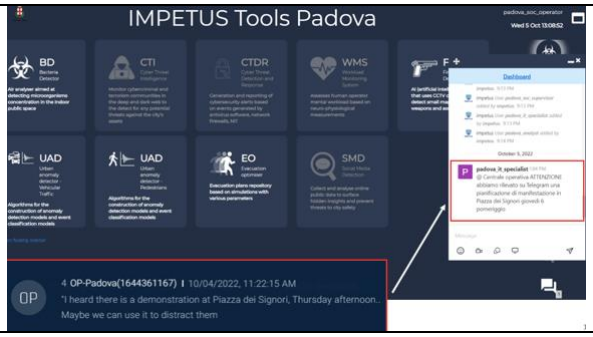
Screenshots from tools	
	
Credentials are revealed on Telegram channel	Communication in the platform

Figure 8: Snapshots from Pizza dei Signori, the SOC and the location with guests/observers.

3.4 Conclusions from the practical trials in Oslo and Padova

The trials carried out in both cities were complex and involved evaluation of multiple aspects of many different tools, interactions, and operational issues. Evaluation was further complicated by the fact that the evaluation in Padova did not have the same basis as the evaluation in Oslo. There are two main reasons for this: (a) The tools and platform under evaluation had matured from one Live Exercise to the other; (b) Lessons learned in Oslo about how best to conduct a Live Exercise were implemented in Padova, in some cases leading to more positive outcomes. All of this is reported in full detail in project deliverable *D7.3 "Report on the use of the technical platform in pilots"*. In this chapter, we provide the main highlights of the validation work.

The overall conclusion from the work is that:

- All the tools were judged to be providing valuable capabilities and working (more or less) correctly.
- Roles and competences for each tool were well understood as a result of carrying out the trials.
- The core concepts of IMPETUS address the challenges observed in daily security operations.
- It was highly evident that use of IMPETUS contributes significantly to increased situational awareness, and this has a positive impact on operations.

Lessons learned from the trials are documented in detail in project deliverable D7.3 *"Report on the use of the technical platform in pilots"*. Chapter 5 below provides a summary of key lessons learned in the various phases of the project, including lessons from the validation work carried out in the cities.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

4 Project contributions to state-of-the-art/practice

In this section we describe the main contributions of the project, especially in terms of functionalities provided. These advances also suggest potential for practical adoption and evolution of the state-of-practice in ensuring safety in public spaces in smart cities. The main contributions of the project can be categorized in two major types:

1. Increased urban security capabilities: new technological capabilities developed and integrated in a common platform in order to support various actors in the conduction of security operations in the cities. More details are provided in the table below.
2. Increased awareness about implementation issues: increased knowledge of key issues and approaches related to ethics, data privacy, practical operations and cybersecurity. The main contribution of the Practitioners' Guides is the development of a centralized and public resource aimed at potential adopters as well as developers and researchers, including educational material and guidance critical to the implementation of urban security technology. The ambition of such resource is to improve understanding and facilitate dialogue between the respective areas of knowledge and practice.

The following table summarises the technical advances made (with respect to the status at the start of the project) for each of the key technical results of the project.

AREA/TECHNOLOGY	IMPETUS CONTRIBUTIONS

Automated weapon detection from CCTV images: the IMPETUS **Firearm Detector**.	• Significant reduction in number of false positives.
	• Detection of different kind of guns (including small ones) and rifles
	• Development of synthetic data, making it possible to train the AI without the need to gather footage of real people holding guns. This vastly improves the task of training the AI because:
	  ○ It is easy to define a wide number of different scenarios and re-play these multiple times for training purposes.
	  ○ Concerns about personal data (and the administrative work needed to address these) are eliminated completely.
	• Development of a dedicated UI.
	• Telegram integration to share information (image of the gun holder, geo-localization and short video) with security personnel in the field.
	• Automatic generation of additional alarms.
	• 2 patents registered.

Automated detection of abnormally high concentrations of bacteria: the IMPETUS **Bacteria Detector.**	• Improved collection of aerosol to improve sensitivity of the device • Development of a dedicated UI. • Integration with Telegram: the SOC operator can quicky share information (position, level of bacteria detected) with specialized first responders by just clicking a button. • In the sequence of the analyse, developed an alternative way to conserve the sample in case of alert to facilitate the specific analyse by the rescue service • Potential/partial integration with Urban Anomaly Detector.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

AREA/TECHNOLOGY	IMPETUS CONTRIBUTIONS
Using AI to detect abnormal situations that may be a cause for concern: the IMPETUS **Urban Anomaly Detector**.	• Development of anomaly detection algorithms that can be applied to a very wide range of potential datasets, • Algorithms tested over a long period of time on large volumes of real-world data: pollution and pollen levels; positions of buses (Oslo); number of cars entering/leaving city centre (Padova); number of pedestrians entering or leaving Piazza dei Signori (Padova). • Functionality demonstrated through detection of a genuine anomaly connected with a real attack (shooting in Oslo bar, June 2022, leading to traffic congestion involving 9 buses during nighttime).Development of 3 dedicated UIs. • Improved capability to describe the measures that appear to be more anomalous than others, giving a perception of the variables that mostly contribute to the anomaly. • Implementation of an automatic approach to regulate the sensitiveness of the algorithm in detecting anomalies.
Spotting online messages that may indicate possible trouble or threats: the IMPETUS **Social Media Detection tool**.	• Tool applied to analysis of real cases. • Improved visualization and graphs. • Improved capability to detect and distinguish positive vs negative sentiment (improvement arose to deal with issues that arose during testing in Padova acceptance pilot). • Improved capability to detect “ironic” positive posts. • Improved capability to detect online threats against the cities.
Providing advice to manage evacuations in emergency situations: the IMPETUS **Evacuation Optimiser.**	• Improved simulation criteria (improvement arose to deal with issues that arose during testing in acceptance pilots). • Definition of relevant potentially dangerous situations (after interviewing different kinds of first responders that confirmed the assumptions related to people behavior during an emergency or panic-related reaction). • Extended scope from specific situations (related to the actual context) to guidelines that could be applied more generally. • Development of a dedicated UI to visualize (prerecorded) simulations.
Detecting and mitigating threats from cyber space: the IMPETUS **Cyber Threat Intelligence tool.**	• Real analyses carried out and real threats detected. • Improved awareness of end-users/IT specialists. • Potential impact on current cybersecurity processes/procedures in the two pilot cities. • Developed new/different countermeasures and points of attention.
Detecting vulnerabilities in IT infrastructure: the IMPETUS **Cyber Threat Detection and Response tool**.	• Integration with XM Cyber tool (abandoned after departure of partner from consortium). • Developed revised approach, including integration with NESSUS tool. • Improved capability to find the best “point of intervention” (countermeasures effective if the corrective intervention has been undertaken on the right node of the assets network). • Improved adoptable countermeasures. • Development of a dedicated UI.
Monitoring mental workload: the IMPETUS **Workload Monitoring System.**	• Reduced dimensions of the monitoring devices. • Reduced time for adapting the monitoring system to an end-user. • Improved “general monitoring model” usable without adapting/customizing the system. • Developed dedicated UIs for Operators and Supervisors.

This project receives funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883286.

AREA/TECHNOLOGY	IMPETUS CONTRIBUTIONS
Providing common situational awareness: the **IMPETUS Platform.**	In contrast to the other technical results, this tool was developed "from scratch" in the project to provide: • Improved situational awareness. • Improved coordination (among different agencies, among different sectors of the same organization) • Improved usability and information visualization. Improvements to core functionality made in response to experiences testing in the pilot cities: • Developed customized UIs for 6 different personas/roles: to present only information relevant to the role and avoid information overload. • Integration with Telegram messaging app. • Integration with Rocket.Chat.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

5 Lessons Learned

We provide here a summary of some of the main lessons learned from IMPETUS. The lessons learned are organized by project phases / work area and relevance is indicated for two primary audiences:

- **PA**: Potential Adopters of the type of technology developed in IMPETUS.
- **DR**: Developers/Researchers who might like to carry out other research and development work in this area in new projects, and perhaps build upon the results and experiences from IMPETUS.

PROJECT PHASE	LESSONS LEARNED	PA	DR
Requirements gathering	A centralized collection led to a very large number of requirements due to the breadth of the topic, diversity of expected results, and variety of aspects considered. Such list of requirements is cumbersome to manage over the course of the project (e.g., to track or revisit individual requirements, or reach consistency across the set).		**X**
	The requirements' gathering phase is an opportunity for partners to be exposed to a large set of needs and challenges in a very multidisciplinary project (e.g., beyond their areas of expertise).		**X**
	It is useful to consider a set of requirements as a "living document", as knowledge about needs and challenges evolves over the course of a project.		**X**
	Typically, the end users or the potential adopters do not know precisely what they need. Their involvement in requirements gathering should be addressed with through a user centred approach (e.g., building from user stories) and incrementally in an agile-style process (e.g., sharing mock-ups as early as possible and improving them according to periodic input).	**X**	**X**
Development: Technology	End users and/or decision makers can be overwhelmed by technologies (they can feel lost or unable to manage them). It is important to find practical examples to let them know -as early as possible- what advantages the technology brings. We learned the importance of comparing "without IMPETUS vs. with IMPETUS". This kind of information should be included in the Communication Plan. We do not expect end-users to contribute significantly to technical development but a deeper involvement in the development process allows them to provide useful input and feedback about areas requiring focus.	**X**	**X**
Development: Practitioners Guides	Interactions with stakeholders confirm the interest of end-users for the kind of guidance and information provided in the Practitioners' Guides; implementation issues (the three pillars of operations, law/ethics and cybersecurity) are critical in relation to societal security technology.	**X**	**X**
	There should be a structured plan for maintenance and exploitation of the Practitioners Guides: this kind of outcome can be a very useful input for future research.	**X**	**X**
Technical integration	The "integration" into a single platform covers aspects that have significant differences in terms of needs and challenges: 1. centralizing access to the tools and information in a single platform; 2. communication with the legacy systems; 3. going beyond technical integration (data exchange), and designing for security operations based on combination of capabilities.	**X**	**X**
	Because of the variety of needs between cities and among security actors, the integration should not be seen as a single package, but rather in modular way.	**X**	**X**

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

PROJECT PHASE	LESSONS LEARNED	PA	DR
	A major challenge of integration is to clarify and agree between end users and technological providers data needs, management and representation: what data is needed, what data is available or how it can be collected, how it can be stored and processed, how it can be visualized to support end users.		X
	To do modular integration, it was useful to build on the existing Snap4city open-source platform, as well as relying on data connection standards (Kafka and APIs): these choices made it easier to build the final "container". However, in spite of the use of these standards, the heterogeneity of tools, purposes and data sources made the integration a much more challenging process than simply connecting tools to the platform. A potential direction to this challenge is to also develop a common semantic structure to exchange information between the specific tools and the platform.	X	X
	An example of tool synergy in security operations is between CTI and CTDR. These tools have different purposes (and potentially different users): CTI supports the identification of threats (cyber intelligence), while CTDR supports the detection and management of vulnerabilities or events on the network. We investigated how these tools could be integrated, but the development of a viable prototype was not possible during the project. Identifying and designing for such synergies can be very effective in supporting security operations but is challenging (e.g., Are the users the same? If not, do they normally share security information?). When relevant, links can be created directly between tools or through the platform (in particular through the design of the interface).	X	X
Operational integration - stakeholder involvement	More opportunities to train the end users would have made the validation activities go more smoothly. Developers need to integrate such training time in the plan and end-users need to ensure availability of relevant personnel.	X	X
	The core functionality of providing a common interface and therefore increasing common situational awareness is of central importance. But it is important to take account of the fact that different users have different needs and require access to different groups of tools: given the variety of tasks and responsibilities in providing urban security, no single user or organisation needs access to all tools. It is thus needed to involve the variety of security actors to design multiple interfaces presenting different combinations of tools depending on the role of the targeted users.	X	X
Technical demonstration: testing phase – "Acceptance Pilots"	The multiple test and validation events organized in the two cities helped drive and orient the development of the results by providing many opportunities to collect feedback and input from end-users (operators and managers) at different levels of maturity.		X
	One of the main lessons learned from Acceptance Pilots (APs) was that the SOC operators were not the only potential end users. After the APs, we proceeded with developments considering 6 different kinds of end-user roles.	X	X
	Technical testing activities should involve first and foremost developers and end users. Other kinds of stakeholders could be involved as observers, but involving them likely requires significant effort (better to do at a later stage with more tangible results).	X	X
Technical demonstration: validation phase – "Live Exercises"	Technical validation activities should be kept separated from communication and/or dissemination activities as much as possible: mixing them can cause confusion, frustration and ineffectiveness (e.g., create conflicts between objectives to test the results and to showcase them to potential adopters).		X

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

PROJECT PHASE	LESSONS LEARNED	PA	DR
	The benefits in terms of information sharing/common situational awareness would be even greater if the IMPETUS platform could better integrate the multiple existing tools (legacy systems) used in the cities.	X	X
	The alerts provided on the platform helped operators become aware of situations needing attention and make decisions about what steps to take. But further refinement is needed to: 1. Prevent the number of alerts becoming overwhelming. (In the trial in Oslo, the lowest score assigned by evaluators was 3/5 for a question about operators being overloaded with too much information). 2. Categorise events (e.g., by criticality) to help operators prioritise which event need a response most urgently.	X	X
	Operators experienced that, for the most part, the tools worked the way they are supposed to. Their concerns were more about interfaces and how to fit the platform into operational procedures and practices.	X	X
	It is clear that some kind of training is needed to use the tools and the platform effectively. In initial use, operators sometimes did not understand what the alerts were telling them. There was also a feeling that, in some cases, the full potential of the tools was not achieved as operators lacked training and hands-on experience.	X	X
	People still want to *talk*. The "chat" function was useful, but the need for verbal communication remains, and has to be achieved using totally different legacy means. It would be useful if this could be provided within the platform.	X	X
Project promotion	The "final dissemination event", although taking place at the end of the project should be planned from very early stage and presented as a key project target for which 100% commitment is required of all partners.		X
	It is very useful to look for synergies (similar projects, other organizations interested in the same topics) to share efforts and reach wider audiences.		X
	For such a broad and potentially complex topic, videos (even short and/or not technically perfect) can be a powerful communication medium for many project activities and outcomes. Videos could include interviews (also to share the status of the work), "backstage" insights with partners explaining difficulties and solution to problems, external stakeholders' impressions.		X
	The results booklet with the one-pagers for each results proved useful to quickly capture the attention, understanding and involvement of external stakeholders.	X	X

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

6 The way forward after IMPETUS

6.1 Demonstrating feasibility and moving towards interoperability

IMPETUS has demonstrated the feasibility of using technology (supported by Practitioners Guides) to significantly improve security in public spaces. Decision-makers in the two pilot cities are already convinced of this. The project's communication activities, and its COSSEC network, have been making progress in spreading this message more widely.

At the close of the project, some of the results are already available for use as commercial products (or soon will be), some are available for free – and some need further development (see next section for details). But it would not make sense to portray IMPETUS as a "one size fits all" solution for technological support for urban security. Other tools/approaches are under development, and others will surely emerge in the future. The most promising strategy to benefit from IMPETUS must surely be to encourage interoperability, so that urban security tools from different sources can work together in different systems, also integrating with legacy systems.

As a first step in looking into the potential for future integrations, IMPETUS has co-operated with our "sister" project S4AllCities[4] – a project that ran in parallel and produced a solution that has a great deal in common with IMPETUS. We together created a classification of the different types of functionalities needed to support urban security and mapped this to the tools produced in each project. The mapping clearly shows that the overall scope for the type of support needed is rather wide, that the two projects sometimes overlap – but in many cases complement each other. From this we conclude that promotion of a wider ecosystem is a promising way forward.

6.2 Availability and future plans for the IMPETUS results

In the table on the following 2 pages, we present the following information about each of the project results that were described in Chapter 2:

- Contact information if you want more information or are interested in using the result.
- Current status (product, prototype, licence needed, free, ...).
- Plan for future development of the result.

[4] See: https://www.s4allcities.eu/

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

IMPETUS Results: Status as of 28th February 2023

Result	Contact	Current availability	Future plans
Practitioners Guides	kaaniche.nesrine@telecom-sudparis.eu Institut Mines Telecom	Publicly available, under Creative Commons CCBY-NC-ND 4.0 license (Attribution, Non Commercial, No Derivatives).	The guides will grow and evolve as new technologies arise, bringing new challenges and possibilities. License terms will remain the same.
Firearm Detector	joe@ai-lert.com CINEDIT	Patent protected that requires a paid subscription to share alerts and to have a customised AI model.	Deployment of the firearm detector in different contexts. Development of a knife detector, and - later on - of a suspicious behavior detector.
Bacteria Detector	sandrine.bayle@mines-ales.fr Institut Mines Telecom axelle.cadiere@unimes.fr Université de Nimes	Available through the establishment of a research collaboration project with the institution.	Cooperation with French Firefighters for further development: in particular size reduction and UI optimisation.
Urban Anomaly Detector	michelangelo.ceci@uniba.it CINI	Available through the establishment of a research collaboration project with the institution.	Further development of interesting applications with Italian municipalities. Release a first version of a built-in UI.
Social Media Detection	guillem@insiktintelligence.com Insikt Intelligence	License fee.	Extending the tool to other languages. Developing a new version of the UI, more specific to municipalities. Enter new markets outside Europe.
Evacuation Optimiser	paolo.mocellin@unipd.it University of Padova	Consultancy service. Available through the establishment of a research collaboration project with the institution.	Further development, in particular implementing new features such as auto-generation of scenarios. Provide consultancy activity to stakeholders to optimise evacuation strategies.
Cyber Threat Intelligence	elad@cybersixgill.com Sixgill	License fee.	Search for business opportunities. Improve AI and Machine Learning algorithms.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

Result	Contact	Current availability	Future plans
Cyber threat Detection and Response	joaquin.garcia_alfaro@telecom-sudparis.eu Institut Mines Telecom	Available through the establishment of a research collaboration project with the institution. Background software (https://prelude-siem.org/ & https://github.com/fiware-cybercaptor/mulval) is freely available.	Test on a different urban scenario (sewage treatment). Improve cyber threat mapping algorithms, adding also optimisation factors (e.g., financial impact of cyber threats and attacks).
Workload Monitoring System	johan.deheer@nl.thalesgroup.com Thales	Patent protected. License fee.	Develop a commercial product within Thales Group, in order to then to sell a service.
The IMPETUS Platform	Radu.Popescu@siveco.ro SIMAVI	AGPL license (the same that applies to Snap4City, on which the Platform is based). No other license needed.	Further development of the solution, in order then to sell a service for smart cities who want to adopt a unifying solution that incorporates different tools and functionalities.

Further information about availability and future plans for IMPETUS results is available on our project website at:

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.

The IMPETUS Consortium

SINTEF	SINTEF, Strindvegen 4, Trondheim, Norway, https://www.sintef.no	Joe Gorman joe.gorman@sintef.no
Institut Mines-Télécom	Institut Mines Telecom, 19 place Marguerite Perey, 91120 Palaiseau, France, https://www.imt.fr	Joaquin Garcia-Alfaro joaquin.garcia_alfaro@telecom-sudparis.eu
UNÎMES	Université de Nimes, Rue du Docteur Georges Salan CS 13019 30021 Nîmes Cedex 1, France, https://www.unimes.fr	Axelle Cadiere axelle.cadiere@unimes.fr
cini consorzio interuniversitario nazionale per l'informatica	Consorzio Interuniversitario Nazionale per l'Informatica, Via Ariosto, 25, 00185 – Roma, Italy, https://www.consorzio-cini.it	Donato Malerba donato.malerba@uniba.it
Università degli Studi di Padova	University of Padova, Via 8 Febbraio, 2 - 35122 Padova, Italy, https://www.unipd.it	Giuseppe Maschio giuseppe.maschio@unipd.it
Entrepreneurship Development Centre for BIOTECHNOLOGY and MEDICINE	Biotehnoloogia ja Meditsiini Ettevõtluse Arendamise Sihtasutus, Tiigi 61b, 50410 Tartu, Estonia, https://biopark.ee	Sven Parkel sven@biopark.ee
SIMAVI Software Imagination & Vision	SIMAVI, Complex Victoria Park, Corp C4, Etaj 2, Șos. București – Ploiești, nr. 73 – 81, Sector 1, București, Romania, https://www.simavi.ro	Gabriel Nicola Gabriel.Nicola@simavi.ro Monica Florea Monica.Florea@simavi.ro
THALES	Thales Nederland BV, Zuidelijke Havenweg 40, 7554 RR Hengelo, Netherlands, https://www.thalesgroup.com/en/countries/europe/netherlands	Johan de Heer johan.deheer@nl.thalesgroup.com
CINEDIT INTELLIGENT VIDEO ANALYTICS	Cinedit VA GmbH, Poststrasse 21, 8634 Hombrechtikon, Switzerland, https://www.cinedit.com	Joachim Levy j@cinedit.com
INSIKT INTELLIGENCE	Insikt Intelligence, Calle Huelva 106, 9-4, 08020 Barcelona, Spain, https://www.insiktintelligence.com	Dana Tantu dana@insiktintelligence.com
SIXGILL	Sixgill, Derech Menachem Begin 132 Azrieli Tower, Triangle Building, 42nd Floor, Tel Aviv, 6701101, Israel, https://www.cybersixgill.com	Benjamin Preminger benjamin@cybersixgill.com Ron Shamir ron@cybersixgill.com
Comune di Padova	City of Padova, via del Municipio, 1 - 35122 Padova Italy, https://www.padovanet.it	Enrico Fiorentin fiorentine@comune.padova.it Stefano Baraldi Baraldis@comune.padova.it
Oslo	City of Oslo, Grensen 13, 0159 Oslo, Norway, https://www.oslo.kommune.no	Osman Ibrahim osman.ibrahim@ber.oslo.kommune.no
Institut za sigurnosne politike ISP	Institute for Security Policies, Kruge 9, 10000 Zagreb, Croatia, http://insigpol.hr	Krunoslav Katic krunoslav.katic@insigpol.hr
T S I M E	International Emergency Management Society, Rue Des Deux Eglises 39, 1000 Brussels, Belgium, https://www.tiems.info	K. Harald Drager khdrager@online.no
UniSMART Fondazione Università di Padova	Unismart – Fondazione Università degli Studi di Padova, Via VIII febbraio, 2 - 35122 Padova, Italy, https://www.unismart.it	Alberto Da Re alberto.dare@unismart.it

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.