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

IMPETUS Project Deliverable: D7.3

Report on the use of technical platform in pilots

Dissemination Status: Public

Authors:

Martina Ragosta, Matthieu Branlat, Maria Vatshaug Ottermo, Joe Gorman (SINTEF); Sandrine Bayle, Joaquin Garcia-Alfaro, Keren Saint-Hilaire (IMT); Alexia Comte, Sebastian Courtin (UdN); Claudio Ardagna, Michelangelo Ceci, Chiara Braghin, Paolo Mignone (CINI); Paolo Mocellin, Matteo Bottin (UPAD); Radu Popescu, Laurentiu Dragomir, Dragos Trifan (SIV); Johan de Heer, Thomas de Groot (THA); Joachim Levy, Lyron Bensoussan, Simon Hudd (CINEDIT); Sandra Cardoso, Maria Mirada (INS); Ron Ofer (SG); Bruno Bonomini, Arianna Dissegna, Stefano Baraldi (CPAD); Ian Simon Gjetrang, Osman Ibrahim, David Røttingen, Magnus Devik Borge, Eirik Bærulfsen, Willy Olsen, Jo Lindberg Augestad (OSL); Mišo Mudrić, Jelena Radosevic (ISP); Brian Holecek, Thomas Robertson, Jaroslav Pejcoch (TIEMS); Alberto Da Re, Manuela Soccol, Gianluca Perillo, Alessio Caneschi (UNI)

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.

About IMPETUS

IMPETUS (Intelligent Management of Processes, Ethics and Technology for Urban Safety) is a Horizon 2020 Research and Innovation project that provides city authorities with new means to improve the security of public spaces in smart cities, and so help protect citizens. It 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.

IMPETUS provides a solution that brings together:

- *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.

Technological results are complemented by a set of *practitioner's guides* providing guidelines, documentation and training materials in the areas of operations, ethical/legal issues and cybersecurity.

IMPETUS places great emphasis on taking full and proper account of ethical and legal issues. This is reflected in the way project work is carried out, the nature of the project's results and the restrictions imposed on their use, and the inclusion of external advisors on these issues in project management.

The cities of Oslo (Norway) and Padova (Italy) have been selected as the site of practical trials of the IMPETUS solution during the project lifetime, but the longer-term goal is to achieve adoption much more widely.

The work is carried out by a consortium of 17 partners from 11 different EU Member States and Associated Countries. It brings together 5 research institutions, 7 specialist industrial and SME companies, 3 NGOs and 2 local government authorities (the trial sites). The consortium is complemented by the Community of Safe and Secure Cities (COSSEC) – a group established by the project to provide feedback on the IMPETUS solution as it is being developed and tested.

The project started in September 2020 with a planned duration of 30 months.

For more information

Project web site: https://www.impetus-project.eu/
Project Coordinator: Joe Gorman, SINTEF: joe.gorman@sintef.no
Dissemination Manager: Harald Drager, TIEMS: khdrager@online.no

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.

Executive Summary

This deliverable is about the usability of the technologies and platform in a realistic scenario and the impact on security and emergency organisations. While the cities developed initial scenarios based on the acceptance pilots, the entire consortium contributed with fine-tuning them.

The project's approach was to use every single test from the acceptance pilots, the intermediate tests and the live exercise and utilize previous experiences into the next. This meant that the Padova Live Exercise would already be using input from the Oslo Live exercise, facilitated by a bridge meeting where all partners contributed.

Both t Padova and Oslo have overall similar goals for their urban security, however for the municipalities there are different operational contexts.

In Italy policing is both a state and municipal task. Italian municipalities have their own local Police, while in Norway, Police is solely a state enterprise. This affects how operations can be performed in the cities, which was reflected in the scenarios, that have some adjustments between the cities.

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 at two primary locations and several supporting ones.

It was observed in the Oslo live exercise that usage of the IMPETUS platform led to several benefits. It was successful in addressing new challenges based on new capabilities. The playback of the data from the exercise indicates that some measures were implemented because of heightened situational awareness, and some were implemented faster than expected.

Outcomes from the Oslo Live Exercise were carefully analysed on several occasions before the Live Exercise in Padova by the consortium, and several areas of improvements were identified and implemented.

The Padova live exercise created a large complex scenario involving multiple actors focused on the Piazza dei Signori square in the centre of the City, spanning across 2 events over two days.

In the Padova live exercise the tools, integrated within the IMPEUS platform, were able to provide additional information and automatically generated alarms that provided increased situational awareness and let the end users take better and quicker decisions concerning response to an emergency or an urgent dangerous situation.

Both live exercises provided valuable experience and insights:

- All the tools were judged to be providing valuable capabilities
- Roles and competences for each tool were better understood
- The concepts of IMPETUS address the challenges observed in operation
- The increased situational awareness and operational impact were evident

The perception in the consortium and from the external participants is that there is evident potential in IMPETUS to increase performance in security and emergency organisations by utilizing the technologies in their operations.

Overall, the Live Exercises were successful in their missions of: (a) stressing the potential value and the potential challenges in uncertain conditions of using the platform and tools; and (b) assessing the potential impact on security operations.

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.

Table of Contents

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.

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.

Table of Figures

List of Tables

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.

List of Abbreviations

Table 1: List of Abbreviations

Abbreviation	Explanation
SOC	Security Operations Centre
FD	Firearm Detector
BD	Bacteria Detector
CTI	Cyber Threat Intelligence
CTDR	Cyber Threat Detection and Response
WMS	Workload Monitoring System
UAD	Urban Anomaly Detector
EO	Evacuation Optimizer
SMD	Social Media Detector
PG	Practitioners Guide
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
LEx / Live Ex	Live Exercise
KOSS	Kommunenes koordineringssentral / Municipal Coordination centre
CSIRT	Cyber Security Incident Response Team
IL	Innsatsleder /Incident manager

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.

List of Definitions

Table 2: List of Definitions

Term	Definition/explanation
TRiO	A system used on Oslo that positions resources connected in time and location, allows for operational command and control and communication with other operations connected to the system.
CBRNE	Chemical, biological, radiological, nuclear and explosive protective measures taken in situations when hazards may be present
KOSS	An effort between three municipalities, managed by the City of Oslo to increase coordination with first responders and other actors. KOSS is located in the Police operations centre.
List of main results from IMPETUS, with brief descriptions	
Practitioners Guides	Documentation that brings the lessons learned from IMPETUS to a wider audience
Firearm Detector	Continuously monitors CCTV feeds and automatically creates an alert if a firearm is detected in a public space
Bacteria Detector	Continuously monitors air samples to detect abnormally high concentrations of airborne bacteria
Cyber Threat Intelligence	Detects, classifies and helps mitigate cyberspace threats to an organisation's IT assets
Cyber Threat Detection and Response	Detects cyber vulnerabilities in IT Systems: raises alerts and suggests countermeasures if they arise
Workload Monitoring System	Continuously monitors surveillance camera feeds and automatically creates an alert if a firearm is detected in a public space
Urban Anomaly Detector	Continuously monitors data gathered from multiple city sensors and detects cases deviating from the norm - indicating possible cause for concern
Evacuation Optimizer	Provides instant advice to emergency staff on how to effectively manage an evacuation, based on simulations of different evacuation scenarios
Social Media Detector	Scans large volumes of text on social media and other public online sites, looking for topics/keywords that might indicate potential trouble or threats

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 About this deliverable

1.1 Intended readership/users

This deliverable provides an overview of what happened before and during the Live Exercises in pilot cities Oslo and Padova and, moreover, feedback collected during the exercises (mainly from the end users) and following analysis made by partners and other stakeholders.

The document provides valuable input to the Practitioners Guides. The document is public to everyone, however, the readership will largely be those that need detailed information about the process and end results, such as:

- project partners
- cities
- other stakeholders
- COSSEC members

1.2 Why would I want to read this deliverable?

The readers will have an overview of the work the consortium partners undertook before and during the Live Exercises, validation of the tools and operations by scenario-based exercises, improvements from the acceptance pilots and learning point from the Live Exercise. The document will provide valuable insights for the Practitioners Guides and organisations that wish to make use of the IMPETUS platform and tools.

1.3 Structure

This document is structured in 4 parts, that should help the reader to understand the "journey" made to undertake a fair and objective evaluation of what the Consortium have developed.

These 4 parts are:

- a general introduction
- details about the preparation phase
- information to understand what occurred during the Live Exercises and how the evaluation has been done
- comments on the outcomes.

1.4 Other deliverables that may be of interest

As D7.3 reports on the use of technical platform in Live Exercises, several deliverables may be of interest:

- D1.2 to understand requirements and to have a clear idea of what and why has been tested
- D2.1 to be aware of IMPETUS platforms features and its state of development
- D3.1 to be aware of IMPETUS tools features and their state of development
- D6.1 for initial concepts of operation of the SOCs involved in the Live Exercises
- D7.1 for the methodology and criteria's concerning validation
- D7.2 for the report of results and learning points from the initial validation exercises (Acceptance Pilots)
- D7.5 for the platform focused initial cyber vulnerability report from the Acceptance Pilots
- D8.4 for observations and workshops
- D11.1 – D11.7 all deliverables for ethical aspects related to work done in the project
- Practitioners Guides

1.5 Synergy with other projects/initiatives

The Live Exercise in Oslo was able to include two projects, one internally in Oslo and one collaborative.

From these projects there were two primary tests that were integrated into the live exercise.

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.

- TRiO

An Oslo municipality project, where a technical test of the systems' capacity and some new functionality was performed.

- Evacuee and next-of-kin centre

The exercise focused on new procedures and technical systems in a collaborative project.

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.

2 Planning

2.1 From acceptance pilots to live exercises

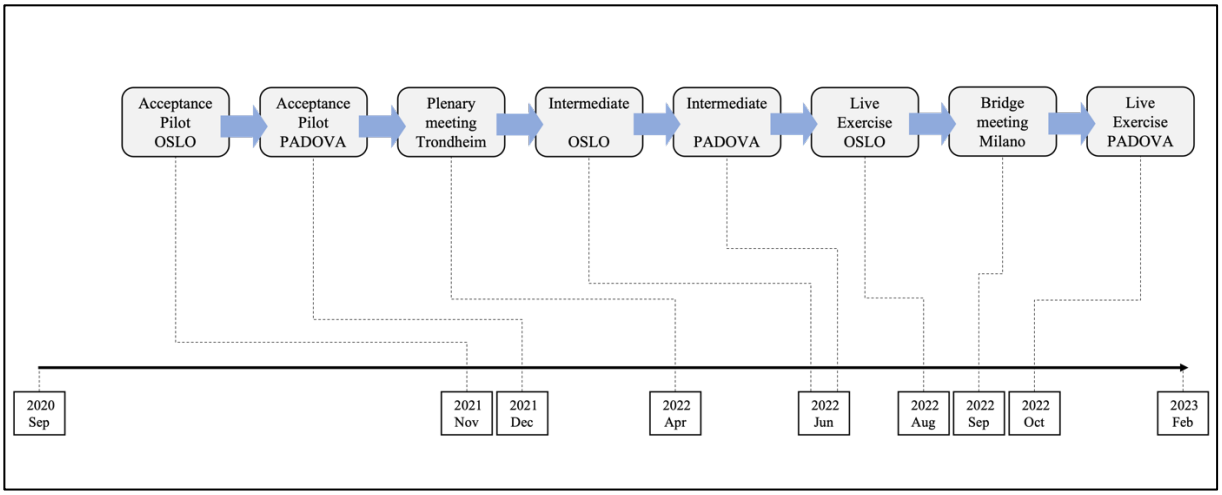


Figure 1 Timeline

As shown in figure 1, the validation process has been quite complex.

The first official touch base for the Consortium partners has been the 2 Acceptance Pilots. These two events were aimed to check the status of the developments according to the DoA, the requirements drafted at the beginning of the project's activities and the validation plan.

The cities were satisfied with the technologies and the capabilities they provided. After the Acceptance Pilots, the cities and technical partners have been working together to adjust the tools to their local needs. The most significant changes have been the Evacuation Optimizer and Cyber Threat Detection and Response, which were revised concepts developed in IMPETUS after changes to the original ones.

For the acceptance pilots, the platform was only a prototype. It has seen a lot of development in every aspect from system control, communication with tools and UI. This has been a collaborative process where both technical partners and end-users have had several needs to be fulfilled.

Some meaningful and helpful feedback have been collected, as reported in D7.2. In particular, it become clear that the potential end users of the tools would include more than just SOC operators.

The description of six kinds of potential end users has been shared during the Plenary meeting in Trondheim (see also D3.4), and according to this deeper insight, raised the need for a customizable platform able to provide the right set of information to the right potential end user.

The two Intermediate meetings have been planned with the aim to collect further indication from the field: cities indeed have different safety and security equipment. Here have been undertaken some tests aimed to verify if the tools were able to collect data from the local sources (e.g. sensors, CCTVs, etc.) and transform them into useful information and adding alarm for the end users.

The tools' container, the s "IMPETUS platform", needed some important improvement to let the end users use the tools in a more efficient way.

The Live Exercise in Oslo was been the first "final exam": as reported in this document, even if it was clear that the developments had been undertaken in the right direction, several impacting feedbacks have been collected for the last final exam, the Live Exercise in Padova. To speed up the fine-tuning process, a "bridge" meeting has been undertaken to deeply analyze the first outcomes.

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.

2.2 General description of planning activities

The planning activities for the live exercise have had several interests and necessities. Both cities have also had intermediate exercises between the acceptance pilots and live exercises. The intermediates were functionality testing of the tools and platform and required that the planning phases needed to achieve this has been finished before the live exercises in order to be able to reduce the chance of technical issues and solve what has been discovered before the live exercises.

From the acceptance pilots in the cities there have been many efforts between several partners to develop on the functionality between the tools and the platform, the platform and the end user and between the end user and the tools. Some tools also have possible synergies to be exploited which some partners have pursued.

The cities scenario processes have been complex processes that have needed to take into account the realism of the scenarios, the sequencing, the tools capabilities, and also involvement of external actors and their interests, opportunities and capabilities in the scenario. The cities have also had processes for facilitation which amongst other involve planning of location for live exercise and visitors, activities for the live exercise and consortium, practical needs for partners, scenario requirements to location, staffing and technical aspects amongst others.

The intermediate tests in both Oslo and Padova provided useful insight to the planning of the live exercises, as the live exercise planning was well underway at the time of the intermediate. Apart from some technical difficulties at the intermediate tests, it gave a good understanding on how the integration between the tools on the IMPETUS-platform would contribute in the live exercise. One specific point of interest from the intermediate was that it became clear, in terms of software development, it was necessary to focus more on the integration between the tools and the platform, as well as focus on the user interface.

These activities are in addition to the planning activities in work package 7 and task 7.3. The evaluation structures in task 7.3 have also had meetings with D7.1 contributors. The goal of these meetings was to understand better how to apply the D7.1 in a live context during the live exercises. In addition, the normal project structures such as the monthly plenary meetings and board meetings has discussed several aspects in the planning phases.

Outside of the work in the defined tasks in the work packages, there have been established working groups dedicated to contribute to solving specific issues of scenarios, develop on user profiles and personas, UI and platform developments.

2.3 Planning Oslo and Padova Live Exercises

Both City of Padova and City of Oslo have overall similar goals for their urban security, however for the municipalities there are different operational contexts.

In Italy policing is both a state and municipal task. Italian municipalities have their own local Police, while in Norway, Police is solely a state enterprise. This will affect how operations can be performed in the cities, which will be reflected in the planning phases and scenario which have minor adjustments between the cities.

In example, while for the exercises in Padova the partners had the opportunity to manage also some real data, because directly supervised by the Local Police, in Oslo instead it was mandatory to use only synthesised data.

Managing real data has been in any case always considered a potential issue: both cities preferred to use synthesised data for various purposes, such as training the tools' A.I. and providing data able to produce alerts where real data would have none e.g. when no ongoing incidents.

For instance, especially interesting synthetic data have been developed with the aim to train the Firearm Detector: instead of recording real people holding guns in a public (and potentially crowded) place, some small "movies" have been created adding synthetic unreal characters with pictures of real guns in a real empty physical context.

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.

2.4 Oslo scenario development

The scenario in Oslo was developed from the scenario of the acceptance pilot. However, it would need to be refined in several aspects, as some perturbing needs would need to be covered. In particular, realism and stress factors were considered important. The plot of the scenario should be relatable to the current society, as well as the roles and partners involved in the scenario should be exercised in a realistic manner to how they operate. Secondly, it was important that the scenario could facilitate the use of all tools on the IMPETUS-platform in a natural manner. In other words, the backbone of the scenario is to show how the tools on the Impetus-platform would contribute in a real-life event. Naturally, some preconditions were taken, but it is the projects understanding that the scenario is in fact realistic.

In addition to the aforementioned requirements to the scenario, some other aspects were taken into consideration as well. It was necessary to create a scenario in which a security operations centre was at the core of the response management, and not became a policing matter, changing the SOC into a position of being under command of the Police and tools testing could be irrelevant. This was important in order to have an environment in which the tools could work properly as intended. Additionally, to properly test the tools in a realistic operational environment, the scenario needed to create realistic and stressful situations. The scenario does facilitate this aspect, and the stress aspect was further developed in the exercise script. The scenario also needed to be both realistic and suitable not only to the application of the tools, but also for other participating partners relevant in the emergency response. This was important to ensure a holistic, well-functioning and realistic collaboration between all active roles in the scenario.

When it comes to how the scenario was developed in terms of method, workshops have been held frequently. Both formal and informal work meetings did contribute to a steady progress, as well as ensuring that all interested parties had an agreed understanding of the scenario's nature and purpose. There has also been close contact with external parties that participates in the live exercise, to gain their insight and input in regards to the scenario.

The scenario describes what was supposed to happen during the live exercise in general and overall terms. The different events and moments described in the scenario was then developed in an exercise script. This meant that every activity throughout the live exercise were put in order, given a timestamp, responsible actors was designated, communication lines and intentions. This was developed for every activity. Despite having a clear plan, it was also needed to leave a lot of the decision making to the participants in the live exercise, in other words utilize players action. This was important so that realism could be maintained for the actors involved, and to remove elements of preparedness for the involved actors as actions from other actors could necessitate changes in their own response. This would both add to stress factors and realism.

Still, the order of all activities was important, as some activities must happen before other activities can proceed. This is because of the logic of the scenario as some events would migrate the scenario into new phases and annul the previous activities and their relevance. It could thereby forgo exercise objectives if not key activities were an exercise control-staff decision and not left to player action.

2.4.1 Oslo scenario

The scenario in Oslo was constructed to consider the total chain of events in the acute phase to the normalization of an incident. The Live Exercise therefore developed four scenarios to capture this:

- IMPETUS scenario – where the events took place
- Evacuation – the handling and logistics of evacuation
- Evacuee and next-of-kin centre – the immediate follow-up of people affected by the event
- Digital cooperation – Utilizing TRiO to cooperate

The four scenarios were played out as one large continuous scenario, though some changes were needed between the different scenarios, mainly small changes to the background for each separate scenario and some extras had repurposed roles. That was mainly in the transition from the IMPETUS scenario to the evacuation scenario.

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.

Several of the involved actors used TRiO where they had various responsibilities, such as building the plot as the scenario developed, reporting of resources participating in the event, reporting of actions taken in the event and coordinating between actors in the event based on the current situational picture.

There were several physical locations in play in the exercise. Because of this, the exercise became very complex, but at the same time provided an opportunity to exercise coordination and cooperation. The actors involved are introduced below.

IMPETUS scenario validated in Oslo

The live exercise in Oslo depicts a scenario in which the city council hold a council meeting in which they are supposed to reinstate covid-19 measures. Some members of the public have strong opinions against this. The day before, IMPETUS tools detected plans for a demonstration outside City Hall, against the coming covid-19 measures. Police are alerted immediately. It is also detected a cyber threat towards the ICT-infrastructure of City Hall. On the day of the demonstration, police arrive at City Hall before it has started, and sets up security with the security department at City Hall. As the demonstration starts and progress throughout the day, several events unfold. Not long after the demonstration has started, it became clear that the demonstration is much bigger and more chaotic than first assumed. City Hall also receives a bacterial attack threat via an anonymous phone call, which raised the need for both intelligence about a potential attack and heightened security.

As the demonstration was getting more violent and chaotic, a weapon is detected within the demonstration crowd. Shortly after the weapon detection, police apprehend the suspect. Minutes later, a bacterial attack was detected, which also triggered the fire alarm due to smoke from the device in which the bacteria were contained. The Fire and Rescue agency would normally respond to a biological contamination event from their Fire and Rescue agency's predetermined response plans. Due to Fire and Rescue operational needs outside the IMPETUS projects' control, the Fire and Rescue agency were on site beforehand.

An evacuation of City Hall were ordered, which also made it necessary to end and disperse the demonstration because the demonstration is blocking the main door of City Hall. When the demonstration was ended and dispersed, the IMPETUS-live exercise ended and moved onto the evacuation scenario. See section 3.2.1 for timeline.

Tools

All the tools played their part in the crisis management through the scenario. CTI, CTDR and SMD will be used "the day before" for detecting the demonstration and intelligence, while EO was used subsequently to plan for the demonstration following the next day. UAD gave information during the live exercise about the flow of people, providing alerts when the number of people was drastically rising. CTI was used for forensics when two surveillance cameras stop working, and SMD was used to investigate the bacterial attack threat in social media. FD and BD was used for respectively detecting the weapon in the crowd, and the bacterial attack. WMS was used throughout the scenario, monitoring the mental workload of the SOC-operators. TRiO was used by City Hall SOC to receive and send communication with all other TRiO actors. City Hall SOC had TRiO directly in the platform interface.

Evacuation scenario

As the evacuation of City Hall progressed, the live exercise entered a second phase, which was a municipal exercise. Some of the volunteers playing demonstrators was given the roles as employees of City Hall, and was evacuated to an evacuation and next-of-kin centre in city district of St. Hanshaugen by a bus provided by the public transportation authority RUTER. The goal of the evacuation scenario was to train the actors responsible for the evacuation processes. This was an identified need based on real events where rights to procure had been vague to several involved actors due to the various types of events and implementation of evacuee and next-of-kin centre.

During the evacuation, security personnel using TRiO would accompany the transport vehicle. This would track the movement of the evacuation bus and the personnel would report departure and arrival.

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.

During the evacuation scenario, multiple extras were instructed to call the Police emergency phone (specific exercise number) to provide various pieces of information and try to overload the police SOC with a large scale of callers and information.

Evacuee and next-of-kin centre
The evacuee and next-of-kin centre scenario started before the evacuation scenario. The decision to establish an evacuee centre and where to establish it proceeds an evacuation process. The decision of establishing an evacuee centre is also a simultaneous process with deciding a need for evacuation.

An important exercise objective was the process of establishing the evacuee centre. The exercise called for an evacuee centre established by a city district, a local centre. This have been shown by practical experience being more challenging than a central centre – an evacuee centre that is established by the agency for health. At the centre, they exercised both registration which is needed due to "missing persons from City Hall caused by fire", and psychological support.

Digital cooperation
KOSS, a municipal coordinating centre located in the Police operations centre, used TRiO directly in the platform interface as City Hall SOC and was responsible for the information and resource coordination with the police SOC. TRiO staff ensured plotting of the incident throughout all the scenarios in addition to the overall responsibility of information and resource coordination.

The City Hall had several security guards connected to TRiO as tactical resources. Agency of emergency planning had tactical personnel in the evacuation and evacuee centre connected. The harbour authority and the City Wardens was also connected to TRiO with tactical personnel.

The City Hall, KOSS, City wardens, the harbour authority and agency of emergency planning actively sent information messages building situational awareness across multiple municipal agencies.

The City Hall, KOSS and agency of emergency planning were active users of the operational back-end digesting and supplying information in messages, plot building, in addition to resource overview and management.

This scenario spanned across all scenarios, where different goals were:

- Sharing of information
- Plot building
- Joint situational awareness

Roles during the exercise
There were multiple actors involved in playing out the scenario and the planning phases towards the live exercise.

- The consortium was involved in the planning of the exercise from scenario development to participating as exercise evaluators, observers and providing tool support during the scenario in case of need for back-up solutions.
- The City Hall General Services are responsible for the security services. They provided the SOC, operators, personnel for crowd control, extras for the exercise and exercise location.
- The District of St.Hanshaugen provided a fully staffed evacuation and next-of-kin centre and exercise control.
- The Agency for Health provided exercise planning and control for the evacuee centre scenario in addition to evaluation.
- The Police provided on site incident manager, personnel for crowd control, a fully staffed evacuation and next-of-kin centre in addition to exercising their entire on-duty SOC and internal exercise control.
- RUTER provided the public transport services for the evacuation process.
- The Emergency Planning Agency provided exercise control staff, KOSS SOC and TRIO staff.
- Agency for Fire and Rescue services provided material and personnel for biological incident response.
- The Agency for Urban Environment provided with city wardens for the evacuation and next-of-kin centre.

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.

- His Majesty's The Kings Guard provided extras for all exercises.
- Several city districts provided extras for all exercises.
- All actors were involved during the planning phases for the live exercise. An important focus during the planning phases was to facilitate the opportunity to create and exercise individual goals for the participating actors, while integrating it in the overall exercise scheme.

2.5 Padova scenario development

Since the start of the project activities, CPAD and OSL has been working together to find a common way to plan and undertake similar actions with the aim to maximize the project outcomes: similar activities would have been comparable in a content of validation and more meaningful also to provide inputs for technical development and improvement of the IMPETUS solutions.

In addition, the Consortium always considered the activities undertaken in the cities as "stages of the same journey": CPAD and OSL planned together, tested firstly in Oslo, collected and analysed feedback, then finetuned in Padova.

According to this, Padova scenario has been initially drafted to be very close to Oslo's with the same objectives: challenge all the tools – within the platform – during a realistic and "complicated" sequence of events.

After the Live Exercise in Oslo, as expected, the collated feedback underlined the need of some changes. See section 3.3 (and appendix A) for more details.

Indeed, the sequence of events of the scenario was divided in 2 different days with the aim to get a more complete involvement of all the potential end users -not only SOC operators- and to let them to practise with the tools that really could improve their own daily job (e.g. Social Media Detection should not be considered a tool for SOC operators).

2.5.1 Padova scenario

The live exercise in Padova depicts a scenario in which some criminals try to undertake a terror attack in the city centre (Piazza dei Signori square) taking advantage of an unauthorized demonstration against further Covid-19 restrictions the City Council is planning to adopt.
Early indications of this demonstration, prepared by some citizens, have been detected the day before, using the IMPETUS Social Media Detection tool. Similarly, some hints about a potential infiltration have been discovered in the dark web using IMPETUS cybersecurity tools, after an unusual cyber-threat towards the ICT-infrastructure has been detected and solved.
The day after, the Local Police raise the alert level and prepared to manage an evacuation in the square; the potential risk is shared with the other Police forces.
An anomalous flow of cars approaching the city centre is detected. In addition, an unusual number of pedestrians are coming into the square: the unexpected demonstration was actually taking place.
While tension in the square is growing, suddenly, an alarm about a bacteriological attack was generated within the municipality building in Piazza dei Signori. The administrative personnel were asked to get out and they merged with the people demonstrating. This causes panic and confusion among the citizens in the square.
In this chaotic situation, three people armed with guns are preparing to shoot in the crowd. One of these guns has been detected moments earlier: the Local Police and the other Police Forces are hence promptly coming and are able to arrest the gun-holders before any shooting took place.

Tools
As for Oslo, all the tools played their part in the crisis management through the scenario. During the first day, the Intelligence Analysts and their supervisor, using the SMD, were able to understand the citizens' general sentiment (rage against the City Council) and they were able also to detect some hints about the possible demonstration. The IT specialists and their supervisor interacting with CTI and CTDR were able to understand that there could have been a criminal infiltration into the demonstration and the likelihood of a terroristic attack was high. These two groups of end users, using the chat of the platform, shared with the SOC operators the detected threats: something "weird could be occur the day after.

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.

According to these inputs, The SOC operators consulted the EO tool to find the best approach to evacuate the square full of demonstrators, in case of issues.
The UAD provided anomalies regarding the flows of cars getting to the city centre and the pedestrians entering the square. FD and BD have been used for respectively detecting the firearms in the crowd (before and during the attack attempt), and the bacterial attack in the municipality building in the Piazza dei Signori square.
WMS, as for Oslo, have been used throughout the scenario, monitoring the mental workload of the SOC-operators.

Municipal exercise
As already mentioned, the Padova live exercise had focused on the involvement of all the potential end users of the IMPETUS solutions more than a parallel/additional exercise in the field.
The municipality personnel working in the offices located in Piazza dei Signori took advantage of the bacteria attack to make their own trial of evacuating the building.
These people then converged in the demonstration, creating panic among the demonstrators: perfect situation for a shooting.
National Police and Carabinieri, the other Police Forces in addition to Local Police agreed to let their SOC operators to join the Live Exercise. So, the 3 SOCs were connected at the same time to the IMPETUS platform and could simulate a coordinated intervention aimed to arrest the criminals holding the guns.

Roles
As for Oslo, there were multiple actors involved in playing out the scenario and the planning phases towards the live exercise.
The **Consortium** was involved in the planning of the exercise from scenario development to participating as exercise evaluators/observers and providing tool support during the scenario in case of need for back-up solutions.
The **Local Police** provided:

- location for meeting the stakeholders
- location for SMD exercise
- Intelligence analysts and their supervisor as SMD end users
- SOC operators and their supervisor as EO, UAD, FD, BD and WMS end users
- Patrols in the field and means to block the cars and pedestrians during the exercise in the square,
- Patrols in the field playing the role of the first responders (arresting the criminals)
- Shooting-instructors playing the role of the criminals
- Volunteers acting as demonstrators

The **municipality** provided authorisations to undertake the exercise in the square

- anticipating the closure of the market that daily took place in Piazza dei Signori
- closing the square and redirecting the traffic to alternative routes

The municipality **IT Department** provided location for the cybersecurity tests and for the exercise activities, in addition to the IT specialist and IT supervisors that attend the exercise as end users of the IMPETUS solutions

The municipality **Demography Department** (based in a building located in Piazza dei Signori) provided volunteers and agreed to combine to the Live Exercise activities to an evacuation test within their HQ.

National Police provided SOC operators and supervisor - connected to the IMPETUS platform – playing their role in an emergency situation and coordinating with the other SOCs to undertake the proper intervention with patrols in the field
Carabinieri – same of National Police

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.

Firefighters – alerted via The IMPETUS platform – provided indications about how to intervene in case of bacterial issue.
Civil Protection Department provided volunteers for the demonstration.

2.6 Platform and tools planning process

In the planning phases of the live exercises, the tool partners carried out a large number of activities. For the live exercises the cities had various needs specific to their organisations, how they operate, how systems and hardware is configured and located, in addition to the specific requirements of the scenarios.

The following tables highlight the main activities that the partners performed in the planning phases towards both City of Oslo and City of Padova.

Table 3 Preparations for Live Exercises

	Preparation for Oslo Live EX	Preparation for Padova Live EX
IMPETUS Platform	For Oslo, all the tools were connected to the platform, including TRiO that is specific to Oslo. Integration tests were performed in order to ensure that data from the tools was well received by the platform. In the same time a new UI concept was implemented. For this a colour code (green/yellow/red) was used uniformly in the UI in order to signal normal/warning/alert situations. A set of dashboards were created using the UI: a central dashboard containing all the tools and tool specific dashboards. A sidebar was also developed in order to show the alerts from the tools in a easy to see way without taking too much space on the user desktop. Communications with stakeholders not directly connected to the platform was achieved using Telegram messages.	For Padova, the platform was integrated with a Padova specific system that monitors the number of people in Piazza dei Signori. 2 dashboards for UAD were created in order to show Padova specific results. The platform was updated in order to show the alerts in real time using websockets (in Oslo a polling mechanism was implemented in order to get new alerts). Small observations related to the UI were implemented. The Telegram integration was implemented in BD tool also

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.

	Preparation for Oslo Live EX	Preparation for Padova Live EX
Social Media Detection (SMD)	For Oslo, without the participation of an analyst during the Live Exercise, the evaluation of the SMD tool would be more inferred and the tool would be used more as a trigger of events than an actual analysis of the tool's dashboard. Since no real data from the sources would contain relevant information for the scenario and it is not ethical to post fake data that could cause disturbances in the real life, there was the need to create a specific dataset with Norwegian posts related to the scenario. The SMD tool had two interventions during the event in Oslo. Therefore, two different datasets had to be created in order to fulfil the scenario of the Covid demonstration and afterwards the event of the biological threat. These datasets were developed with the help of Norwegian-speaking people that gave wordings and phrases with hate speech that were used to create complete posts regarding the scenario.	For the SMD tool, during the Live Exercise in Padova, the Analyst would have access to the SMD tool via the Impetus platform and evaluate the project's content using all the features provided by the tool to get insights related to the scenario. The evaluation of the tool consists of watching the analysts fully use the tool, its usability and its operation. The same as in Oslo's Live Exercise, the objective of the analysis that had to be done with the SMD tool is to detect the day before the Live Exercise that there was talk about the COVID vaccine and certain discomfort and anger and that people were organizing a demonstration for the next day. Since no real data from the sources would contain relevant information for the scenario and it is not ethical to post fake data that could cause disturbances in the real life, there was the need to create a specific dataset with posts in Italian related to the scenario. This dataset was developed in collaboration between native-speaking Italians and people with an understanding of social media to be as realistic as possible. With the Live Exercise objective in mind, the dataset had to contain a wide range of sentiments but focus on hate speech towards the scenario topic and with regards to the demonstration that would take place the next day for the Live Exercise.
Bacteria Detection (BD)	For the Oslo LEx, it was planned in the scenario that the increasing concentration of bacteria in the room would trigger an alert for exceeding the threshold. A room in the basement of the city hall was used for this exercise. An initial message was sent to the platform to inform that the bacteria concentration was normal. For the launch of the alert -exceeding the threshold- some bacteria (safe bacteria) were spread out in the room for 5 min to quickly increase the concentration of bacteria. The objective was for BD to detect an abnormal concentration of bacteria in the room and send the alert to the IMPETUS platform.	For the Padua LEx, unfortunately, only two of our team came to Italy. So, we thought of another strategy to launch an alert when the threshold is exceeded. We developed a comic book simulator to launch an alert. In the scenario as in Oslo, it was planned to send an alert to the SOC operator with a concentration of bacteria exceeding the threshold. An alert was therefore simulated with our simulator DB allowing the operator to test and validate the user interface.

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.

	Preparation for Oslo Live EX	Preparation for Padova Live EX
Urban Anomaly Detector (UAD)	For Oslo, we concentrated our attention on the analysis of sensor data generated from public transport vehicles. In this context, the purpose was to use the Urban Anomaly Detector (UAD) for the identification of anomalous behaviour of vehicles, considering space and time. These data are real data collected in real-time and processed in real-time according to micro-batches. The UAD was trained on historical data that constitute the normal behaviour of the vehicles. The learned model was used during the Oslo Live Ex in order to identify in real-time cases that deviated from the normality. Examples are: i) too many vehicles in an area of the town at a time, e.g., Wednesday at 11:00 am, when such concentration is not expected; ii) unexpected significant delay of some public vehicles in an area of the town where, at that time, this does not happen. For the Live EX we perturbed the collected data in order to simulate such situations.	For Padova, we concentrated our attention on the analysis of data generated from sensors that monitor the traffic in Padova and from sensors that count the number of people (pedestrians) crossing the gates to enter/exit from Piazza dei Signori. In this context, the purpose was to use the Urban Anomaly Detector (UAD) for the identification of anomalous behaviour of vehicular traffic and pedestrian flow, considering space and time. These data are real data collected in real-time and processed in real-time according to micro-batches. The UAD was trained on historical data that constitute the normal behaviour of vehicular traffic and pedestrian flow. The learned model was used during the Padova Live Ex in order to identify in real-time cases that deviated from the normality - Examples are: i) too many vehicles entering the town from some streets in the south-east of the town at a time, e.g., Thursday at 15:00, when such concentration is not expected; ii) unexpected significant flow of people entering into Piazza dei Signori at a time when this does not generally happen. For the Live EX we perturbed the collected data in order to simulate such situations.

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.

	Preparation for Oslo Live EX	Preparation for Padova Live EX
Evacuation Optimizer (EO)	During the preparation step of Oslo Live Ex, a set of reference scenarios for evacuation was prepared. Some meetings with the local representatives were performed to delineate the features of interest for the scenario simulated during the Live Ex. The preparation phase allowed setting the scenario in terms of the number of people involved, triggering event and evacuation geometry. Since no data or counter-person sensors were available in Oslo, additional effort was required to establish a realistic number of people as a definition for the reference scenario, then pre-loaded in the EO tool. A mixed set of scenarios was defined: evacuation of a different number of people from the square and evacuation of groups of people from the city hall building into the square.	During the preparation step of Padova Live Ex, a set of reference scenarios for evacuation was prepared. Differently from Oslo, additional information was available, including reference number of people to consider, restrictions on the public space and rationale of potential initiating events In any case, some meetings with the local representatives were performed to delineate the features of interest for the scenario simulated during the Live Ex. The preparation involved pre-simulating a certain number of reference scenarios (about 50) and formulating related guidelines for optimized response. The guidelines' detail and specific content were discussed with the city's representatives. Working together with the platform developers, some refinements of EO were implemented. These included visualising the evacuation parameters (total evacuation time and coloured risk class) and simplified access to the text file providing the guidelines. Unfortunately, before the Live Ex in Padova was not possible to access the historical data set from counter-person sensors installed at the square gates some months before.
Cyber Threat Detection and Response (CTDR)	For Oslo, the IT specialist would not be able to evaluate the CTDR tool. Moreover, the Oslo team prepared a server where we could install the CTDR tool. Some days before the Live EX, we run the Nessus scan for the assets concerned by the proposed scenario. The output of the Nessus scan was used as input for the CTDR tool.	For Padova, Live Ex, we had a meeting with the IT specialists to show them how to use the tool and how it works. The tool was installed on a virtual machine able to receive traffic information from the Police department network.
Firearm Detector (FD)	For the Oslo LEX, it was planned in the scenario that an attacker located in the camera field of view of the outdoor surveillance camera located at the municipality would pull out a small magazine fed handgun and engage in a shooting position. This weapon anomaly would trigger an alert sent to the platform to inform that a weapon was detected. The objective for the FD tool is to detect a firearm in an open space and send the alert to the IMPETUS platform.	For the Padova LEX, it was planned in the scenario that multiple attackers located in the camera field of view multiple surveillance cameras located outdoor would pull out multiple small magazine-fed handguns and engage in multiple shooting positions. This weapon anomaly would trigger an alert sent to the platform to inform that multiple weapons were detected. The objective for the FD tool is to detect multiple firearms in an open space and send the alert to the IMPETUS platform.

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.

	Preparation for Oslo Live EX	Preparation for Padova Live EX
Work Management System (WMS)	For the Oslo Live Exercise, we concentrated our attention on the analysis of sensor data, generated by the single Operator in the SOC of the City Hall. The City Hall Security Officer would perform his tasks as described in the Live Exercise Scenario. A connector to the KAFKA message broker was created and tested with dummy data in order to connect the alerts generated by the WMS to the IMPETUS platform. For the LEx we collected data two days before the LEX with the operator to calibrate the Workload Monitoring System (WMS) and build a personal workload model. This was done using our custom Workload Calibration Task.	We prepared for the Live Exercise in Padova by configuring the WMS for multiple users in the Padova Police CCTV SOC. Having learned from the Oslo LEx that the operators were already having a high workload during the calibration task due to their active participation in preparation of the LEx, we decided to do the calibration phase a couple of weeks earlier. For this, we visited Padova two weeks before the LEx and collected calibration data from the available operator. These data were used to create the personalized workload model for that operator.
Cyber Threat Intelligence (CTI)	Since our product is a SaaS solution, we did not have to prepare anything special for the Oslo Live EX. We made sure that Oslo's account on the portal and the API integration to the IMPETUS platform were working properly. Moreover, we had a session with Oslo SOC members on how to use the CTI tool.	We made sure that Padova's account on the portal and the API integration to the IMPETUS platform were working properly. We injected fake data into the system in order to allow the IT team to play with the proposed scenario and test the CTI tool capabilities. We had a session with Padova IT team members on how to use the CTI tool.

2.7 Ethical activities

As already experienced for the Acceptance Pilots, during the planning phase leading up to the live exercises in Oslo and in Padova, several ethical and legal considerations had to be done.

The technologies applied in the IMPETUS project do potentially gather many kinds of personal information. Due to this fact, the project was required to deliver an application to the Norwegian center for research data (NSD) and a specific review had to be undertaken by the local DPOs both in Padova and Oslo.

Within the research scope of the project, no objections were raised after assessing the plans for how personal data would have collected, managed and stored. Instead, for any potential real adoption, the cities would be asked to undertake an assessment related to their daily operations.

During the planning phase, there were ongoing considerations on which tools would need synthetic data, and which tools that could be applied with real data.

As already mentioned, not having the Local Police supervising the modalities of data management like in Padova, for the activities undertaken in Oslo an even more strict attention has been paid by the Consortium that decided to adopt only synthetic data.

The project emphasized the importance of informing and involving the participants of the live exercises with regard to what kind of personal data would have been managed. This was done through consent forms with everyone participating in the live exercises and through informing briefing.

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.

2.8 Risks for the live exercises

During the planning phases of the live exercises there were uncertainties concerning some particular issues.

Covid-19 handling was still ongoing in the beginning phases. There was a clear trend of the handling would be reduced as the risks were mitigated through several measures, such as vaccination, quarantining and the extent of severity and number infections were declining. However, the situation was that there were still active measures and handling, and uncertainty connected to how it would develop and how future handling could turn out. This would eventually become clearer, and the risk and uncertainty would become a lower concern, for both the cities.

The war on Ukraine would present new challenges that severely affected the live exercises. The involvement in the live scenario was for a long time uncertain for several actors, as they would be unsure to what resources they would have available to commit. This meant that participation in planning of, and in the live exercise, could be reduced or entirely dropped for some actors.

This affected the planning process of the live exercises. The city of Oslo increased staffing, reducing the dependency on the other actors involved in the live exercise in anticipation of being able to execute the live exercise to its intended scale. The task of planning was also difficult as the understanding of what resources were available for the live exercise would be vague for a long time.

As the summer and the live exercise was coming closer, the scale of the refugee crisis would be considerably lower than estimated and all the collaborating actors in the live exercise were able to participate as intended.

Concerning Padova, a potential risk of having a negative impact on the Live Exercises was related to the local administrative elections that took place a couple of months before the scheduled dates of the exercises.

Indeed, a new Mayor and a new City Council could have caused a different approach to the ongoing activities, could have changed local priorities and limit availabilities of public spaces and administrative personnel (including Local Police officers and operative people) already engaged in the organisation.

Some changes actually occurred (e.g., one of the main project sponsors was no more in the City Council), but Live Exercises could have been undertaken with a limited impact.

Large-scale events dependent on volunteers are sensitive to their ability to participate and to coordinate them, which required a lot of focus from the cities for it to be successful.

Technical support for the live exercises were important due to the methodology of observers located outside of the SOC. In case of loss of connection, these observers would not be able to provide feedback, however there were evaluators present in the SOC. The most significant risk would be loss of connection with the platform which would make connecting to the tools impossible, so this was thoroughly tested in the weeks leading up to the live exercises.

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.

3 The Live Exercises

The Live Exercises have been the last part of the validation process aimed to evaluate the IMPETUS solutions.

As defined in the Validation Plan (D7.1), the validation activities were not focused on the question:

- Do the technologies work?

The technologies in a research project can of course have different level of completeness, so, what has to be assessed is if and how much they are meaningful, if they provide added value.

Indeed, the main validation object is related to the question:

Did we develop/are we developing the right product?

Hence, the focus of the validation is to understand if the solutions are actually USEFUL for the potential end USERS.

Adopting the technologies, end users should undertake their own daily work in a more efficient and effective way, this means:

- Improved situational awareness
- Less time
- Less mistakes
- Improved coordination (meaning a smoother cooperation with different agencies, sectors, first relievers, patrols on the field, etc.)
- Dealing with more accurate information
- Dealing with adding information, not available now

More information is available in the Practitioners Guides.

3.1.1 Methodology

With the aim to undertake an evaluation that can be valid, reliable, robust and trustworthy, we defined a methodology to be used in both the Live Exercises trying to limit any possible bias.

According to the Validation Plan (that is based on the list of the requirements agreed at the beginning of the project development activities and the Grant Agreement), we consider 4 areas of interest:

- The usability of the IMPETUS Platform
- The applicability of the IMPETUS ethical framework
- The impact of the IMPETUS operational framework
- The effectiveness of the IMPETUS cyber security framework

Considering the constraints already faced during the Acceptance Pilots exercises (e.g., the limited number of people allowed to enter in the SOC or the limited availability of the end users due to their critical role), we structured the feedback collection in three phases:

a. Direct observation
b. Restricted interviews with the end users
c. “Public” sharing and Q&A session with the end users

a. **Direct observation**: with the aim to detect the maximum level of details, we involved three categories of observing people: the evaluators, the internal observers, and the external observers.

   Evaluators: a limited number of people (max 3) allowed to sit beside the end users during the Live Exercises sequence of event, asked to direct observe the behaviour of the end users and their interaction with the IMPETUS solutions. They have been asked to fill a specific pre-prepared form and they have been trained about the scenario and the objective of every single event occurring in the exercise, operating with a scale of : Below average, Average, Good, Very Good, Excellent (Appendix B).

   Internal Observers: one representative per partner has been asked to take notes about the whole Live Exercise event and fill a pre-prepared form.

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.

External Observers: all the guests attending the Live Exercise were asked to provide feedback, in particular the COSSEC members have been asked to fill the same form proposed to the Internal Observers

b. **Restricted interviews with the end users:** at the end of the live exercise scenario, the Evaluators interviewed the end users trying to collect the very first and sincere impression
c. **"Public" sharing and Q&A session with the end users**: after the conclusion of the activities related to the scenario, a plenary session took place. Here the end users have been asked to share their feelings, their impression, their suggestions and to answer some questions coming from the attenders.

3.1.2 Research design / Study design

Our research design and overall strategy for answering our validation objectives have focused on observational, qualitative-method study.

To achieve this, all criterion used were linked to the objectives of the IMPETUS solutions as detailed in the Validation Plan (D7.1). The utilized rating process provided as guide to minimise human bias during the evaluation.

This method is considered legitimate and the best approach for answering our overall validation questions.

Our goal, as stated in the validation plan D7.1, is to validate the IMPETUS platform from an end-user perspective regarding usability and operational impact.

Note, that the IMPETUS platform does not log end-user platform interactions, which could have resulted into a quantitative dataset that is up for analyses as well.

3.2 Oslo Live Exercise

IMPETUS as a part of a larger 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. We refer to that below as "the IMPETUS scenario". As noted in detailed descriptions below, that ended around 1145. The overall exercise continued after that (with evacuation with Ruter, evacuee and next-of-kin, Police SOC handling, Fire and Rescue CBRNE and TRiO) until around 1430.

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.

3.2.1 Facilitation and exercise locations in Oslo

There were several physical locations in play in the exercise. Because of this, the exercise became very complex, while at the same time provided an opportunity to exercise coordination and cooperation.

The live exercise took place at Oslo City Hall, with the simulated demonstration in Borggaarden, the square just outside the main exit. The demonstration, which was central in the exercise, was monitored and managed in the City Hall security operations center, and by police and City Hall security services on the outside. Both the Police and Fire and Rescue chose to have one person each located in the SOC for more efficient coordination and information flow. A meeting room in the lower floor of the east tower was used as the site for bacteria release.

The Police operations center was part of the exercise with their SOC located at their main headquarters in Grønland.

Ruter, the public transportation authority, was part of the exercise due to the need for emergency transport from City Hall to the next-of-kin-center in St. Hanshaugen. The order for the emergency bus was received at Ruter`s operations center in the city center, at Ruter's headquarters.

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.

The TRiO-operators, which ran the TRiO-applications, were located at Olav Vs Street 4. A representative from the Emergency Planning Agency in City of Oslo and the developers of the application were present at this location forming the municipal information management function in the crisis management.

The next-of-kin-center was located in a dedicated building in the city district of St. Hanshaugen. The administration from the city district was facilitators of the next-of-kin-center, and collaborated with the police and other relevant actors during the exercise.

The external guests that were participating to watch and observe the exercise stood on a balcony just above Borggaarden, with views over the demonstration while they are being presented live feeds of the tool on screens. A narrator described and commented the exercise while the exercise was running. The goal was that external guests would get a good understanding of the exercise, and how the IMPETUS platform was working. Internal consortium observers were also located at the balcony.

In addition, throughout the week, the entire 9th floor of Olav 5th street 4 was available for project consortium for preparations for the live exercise. The 9th floor consists of 9 meeting rooms of various sizes, including basic facilities such as kitchen, coffee machines and restrooms.

For the day of the exercise, we used the meeting centre in the lower floor of the City Hall where the consortium and external guest gathered for briefings before the exercise and lunch and feedback sessions afterwards. After the feedback sessions all tool providers had stands across two meeting rooms where everyone could see all the technologies in the project and discuss them with the tool partners directly.

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.

3.2.2 How the Live exercise played out

The IMPETUS scenario of live exercise played out as planned, and there were no significant disruptions that influenced the timeline or the events played out.

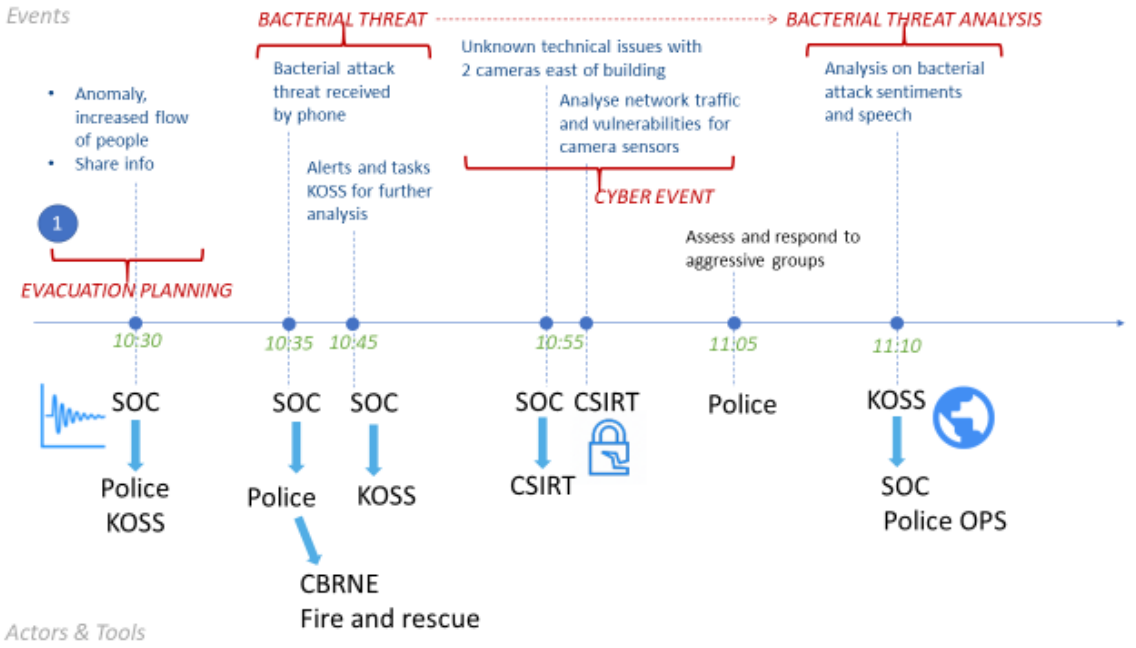


Figure 2 Timeline Live Exercise Oslo 1

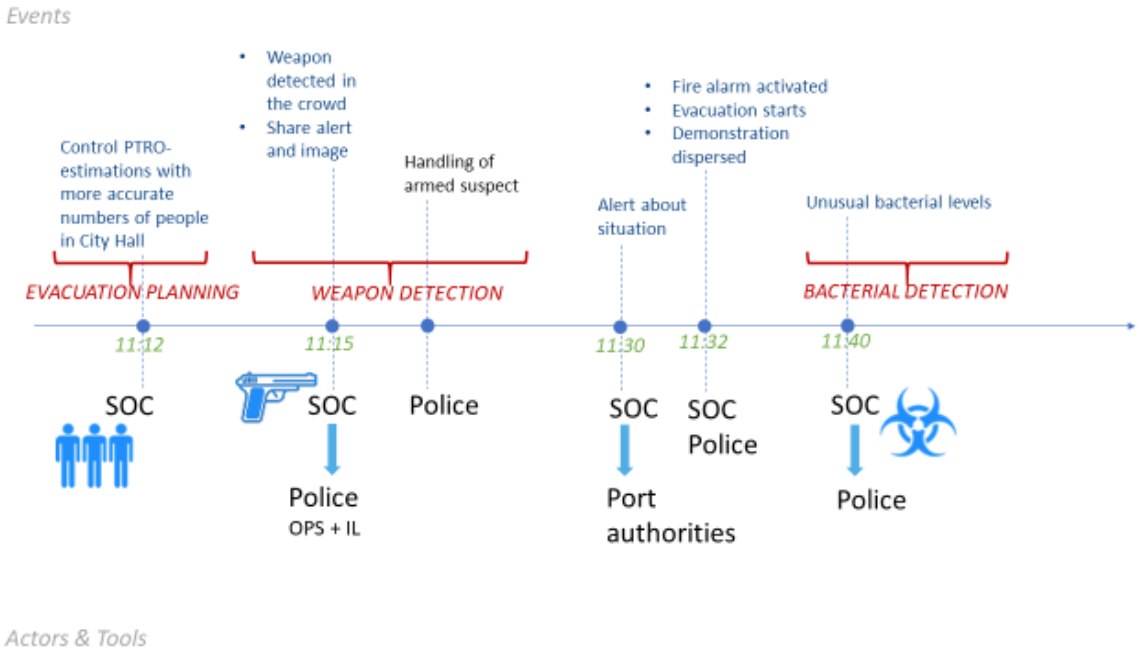


Figure 3 Timeline Live Exercise Oslo 2

The IMPETUS scenario ended around 11:45 and the overall exercise ended around 14:30. The other scenarios (evacuation with Ruter, evacuee and next-of-kin, Police SOC handling, Fire and Rescue CBRNE and TRiO) also played out without any significant disruptions. The figures below (4-7) depict various settings during the Live Exercise.

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.

Figure 4 Inside the SOC

Figure 5 The demonstration

Figure 6 Evacuation bus

Figure 7 Fire and rescue - bacteria decontamination

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.

As can be observed in the figures, the live exercise had many various exercise momentums that provided a high stress situation inside the SOC with hands-on coordination between multiple actors.

3.2.3 Setting

The location of the evaluation was provided by the City of Oslo. The City of Oslo is and has been frequently providing its city as a testbed for innovations in the context of smart city challenges, this includes the security challenges that are addressed in the IMPETUS project but also numerous other challenges related to, for example, energy, logistics, healthcare, et cetera. The SOC provided by the Municipality seems specifically suitable for the evaluation since all the IMPETUS tools could fit into crisis scenarios that may occur around this venue. Also, the Acceptance pilots were done here.

3.2.4 Study Participant SOC operator

The SOC operator was recruited to the exercise just before the Acceptance Pilots and expressed a willingness, including his consent to participate in the Live Exercise. He was selected on the basis of being able to grasp easily the notions of the Project, the potential of the Platform and its Tool, the insight to utilize the information that could be generated from the platform, and where the IMPETUS functions could fit into an operational setting. In addition, he was well trained, fluent in English, curious and open to anything that can support his operating environment, which he himself labelled as challenging. His demographics: 35 years of age, male, Norwegian, trained as SOC operator, 18 years of duty in his role. Our study participant is considered representative of a larger population of SOC operators. The intended sample size at the beginning of our study was a limited number of participants, however, being available for the total duration of the project.

3.2.5 Instruments / Measures

For the evaluation, we used a set of observation questions around usability, ethics, security and operations. This real-time assessment instrument was created for our evaluation purposes but based on some partner experiences on real-time security operation assessments.

For each of the 4 categories (usability, ethics, security and operations) questions were defined based in D7.1, including some evaluation metrics, see Appendix B.

During the evaluator's preparation phase, it became immediately clear that two (ethics and cyber) of the four evaluation categories were difficult to consider from a SOC operator perspective using the observational method we adopted. Therefore, the evaluators concentrated in the usability and operational aspects. Each evaluator took notes during the 1.5 hours crisis based on the utilization by the SOC operator. The evaluators discussed their notes and derived towards an overall observation and take away.

Evaluators

We had three evaluators that were all present in the SOC positioned behind the SOC operator. All three evaluators had a clear view in the interactions the SOC operator had with the IMPETUS platform, which was placed just before him in his operational environment. The reason that we used three evaluators was to minimize evaluation biases. The intended procedure was that the evaluation scorings regarding the questionnaire could be compared and checked on consistency. The evaluators prepared themselves by discussing the exercise scenario and elaborate on the SOC operator expected behaviours as well as the expected behaviours from the IMPETUS platform. Given this preparation, the evaluators had a common understanding of how to interpret the questions in the context of the evaluation in a real-time setting. Evaluators were two females and one male (all partners in the project) with different backgrounds covering technology, human behaviour, and human machine interactions and collaboration. One of the evaluators was Norwegian, which helped with the language barrier when the SOC operator and people involved inside the SOC had to talk naturally.

Procedure(s)/Intervention.

The evaluation took place at August 18, 2022 and lasted 1.5 hours in total. The SOC operator was managing all aspects that were part of the crisis scenario. The SOC operator was in his ‘normal’ environment with other entities involved such as, his supervisor, representatives of first responders (fireman, policeman) that would be normally involved during a crisis management situation or training. The IMPETUS platform was basically an additional screen that provided “Alerts” and “information

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.

items" that he could take into account. Note that the IMPETUS Platform is not part of the SOCs available infrastructure, and is not part of the operational procedures to handle crises. The instruction to our participant was (and given his involvement in the Acceptance pilot) to use whatever is of interest to him to manage the current crisis. Thus, our participant was completely free to utilize the IMPETUS platform, however, he was fully aware that the project was evaluating his use of the platform to deal with the simulated crisis. Note, that one of the tools required our participant to wear a brain computer interface to measure his brain activity for a real-time workload assessment. Our participant had been wearing the brain computer interface before and was comfortable with it.
After the Live exercise, we had a plenary evaluation session the next morning, in which our participant discussed his experience.

3.2.6 Oslo Live Exercise: Overall conclusion and take-aways from the evaluators

The evaluators categorized their conclusions into the following sections:

- Scenario
- Platform
- Evaluation
- Operational
- Usability
- Overall conclusions

Scenario
The evaluators observed that the live exercise overall went as intended and the exercise scenario started on time and finished on time. They could observe that the demonstration scenario for IMPETUS was a part of a larger exercise, which also meant the IMPETUS scope in the context of the overall exercise had to be understood.

Platform
The evaluators observed that the platform worked as intended on a technical level. All the alerts and information generated in the platform was available to the operators, however, the exercise had limited usage of the CTI and CTDR.

Operational
The evaluators noted that the operator did not respond to all alerts immediately, and that UAD alerts were piling up. In the particular case of the UAD alerts the operator knew that the tool was not fully configured causing an excessive number of alerts. However, there was still several times where an alert would be generated, but the operator would not immediately open it. The evaluators observed that the alerts did not grab the operator's attention, and there is a need to work further on how the alerts draw the attention and also the criticality of the alerts.

The evaluators also observed that when the operator would sometimes open the alarm and from there explore the tools further, but that it was unstructured.

It is also noted that the intended users for the SMD is analysts, while in the exercise the SOC operator used the tool.

The operator also had direct access to the WMS tool, however this is intended to supervisors. The operator also said that seeing his workload levels was contributing to increasing stress.

The evaluators noted that the operator used the EO tool several times and that it seems to have been used to gain an idea of how the crowd could move during an evacuation.

The operator did pay attention to the FD alert immediately. The tool had detected a gun, however the gun was a police officers holstered weapon and not the demonstrator's weapon.

The platform did well in supporting the operator's decision-making by providing the operator with information such as the FD alarm, but letting the operator dismiss it as it was a police gun detected.

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.

Communication does however need an overall improvement, as there were multiple channels that the operator needed to use and several different stakeholders present.

Usability
The evaluators also observed that the platform was intuitive to use and that it clearly enhanced the operator's situational awareness in the exercise.

Overall conclusions
The evaluators concluded based on their observations that

- To utilize the IMPETUS platform in the current workflow strict procedures are/become relevant and should be trained.
- Sharing of information is very relevant in an operational context. however, the IMPETUS platform is not (yet) part of the existing infrastructure.

3.2.7 Oslo Live Exercise: Observations tool partners

All tool partners had dedicated personnel to observe the live exercise and provided their feedback in the following tables.

Table 4 Tool partner observations Oslo

	Oslo Live Ex - observations
IMPETUS Platform	There were no technical issues with the platform. The alerts sent by the tools were received and presented in the UI. Telegram messages were sent successfully. Some observations from this Live Ex: update the UI in realtime when new alerts are received by the platform, improve the loading time of some dashboards, make the UI responsive in order to be used on different screen sizes and resolutions.
Social Media Detection (SMD)	In this case, the Covid demonstration dataset was used for the Day-Before section, when an analyst would have reviewed the project shown in the presentation. During the Live Exercise, a new project about the bacterial threat was created in real-time with the correspondent dataset and an alert appeared in the platform. The alert was intended to be sent to the KOSS operator, not the SOC operator which is not an analyst. In this way, the tool was not evaluated during the Live Exercise.
Bacteria Detection (BD)	The Bacteria Detector detected an abnormal concentration after 2 min to spread out the bacteria in the air and sent the alert to inform the SOC operator. The SOC operator shared this message with the CRBN. Indeed, during the LEx in Oslo, the firefighter's department was present for training in case of a biological attack. For us, it was a good exercise because we validated the detection system of the BD, the connexion with the platform, and the end-user interface. The feedback from the SOC operator was good, the information was clear and easy to share.
Urban Anomaly Detector (UAD)	During the Live-EX we perturbed real-time data in order to simulate, coherently with the scenario of the Live-EX, many vehicles showing a significant delay in the area of the Oslo Municipality, which is a symptom of traffic jams (according to the domain experts). The system correctly recognized such data as anomalies, raised alerts, and allowed the SOC operator to contact the supervisor and report on the situation.

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.

	Oslo Live Ex - observations
Evacuation Optimizer (EO)	The Live Ex demonstration in Oslo involved using the EO tool and others provided within the platform. The full potentiality of the EO was not exploited. In any case, the operator(s), both on the Day-Before and during the Live Ex, explored the picture provided by the EO. The EO provided different realistic scenarios following an evacuation and associated practical rules to optimize the scenario and reduce the risk. Using the EO tool, the operator(s) were aware of potentially risky situations that could be used to limit the total number of allowed people in the public space or the choice of specific operative rules to control and reduce adverse consequences.
Cyber Threat Detection and Response (CTDR)	The CTDR tool proposed a countermeasure for the exploited vulnerability from the attack simulation against the CCTV camera.
Firearm Detector (FD)	The firearm detector detected a small magazine fed handgun even though the officer was not engaged in a shooting position. The alert was sent to inform the SOC operator. The SOC operator shared this message with the local law enforcement despite a wrong detection to test the procedures of a verified detection. It was a good exercise because we validated the detection system of the FD tool, the connection with the platform, and the end-user interface. The feedback from the SOC operator was good, the information was clear and easy to share.
Work Management System (WMS)	The Workload Monitoring System calculated the workload of the operator during the LEx scenario and sent the alerts when a high or low workload was detected, to the IMPETUS platform. The system worked as intended during the LEx. There were some problems connecting to the platform but a workaround using a mobile data connection solved this problem. During the scenario there were a couple of alerts sent when the operator was overloaded (high workload) with assignments and information. In the after-action review, the operator confirmed this. The operator told he perceived the WMS as valuable. Not for him directly but for his supervisor, in order to manage the team.
Cyber Threat Intelligence (CTI)	The CTI tool successfully exposed cyber threats against Oslo's municipality and alerted the user on the different threats that were found.

3.2.8 Questionnaires from internal and external observers

Both external and internal observers had the opportunity to provide feedback in questionnaire (see appendix C).

A total of 17 questionnaires were returned, 10 internal and 7 externals. The questionnaire asked the participants to assess a total of 14 questions between the range of "1- not at all" to "5 – very much". There was also the possibility to provide some written feedback, which was utilized by some participants. The table below shows an average of the participants. The external observers would feel it difficult to set marks on the technologies in particular, leading to mostly 2 or 3 respondents giving marks. This makes the marks from the observers very sensitive, so only the internal marks are averaged despite that most of the external marks are averagely higher than the internal. However, the written feedback has been used for this section.

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.

Table 5 Observer Questionnaires Oslo

Question	Internals' mark
Is the IMPETUS platform/tools easy to use for the SOC operators?	3,9
Is the information provided easily understandable?	3,6
Question	**Internals' mark**
Do the IMPETUS platform/tools overload the SOC operators with too much information?	3
IMPETUS platform	3,5
UAD	3,6
CTI	3,8
CTDR	3,3
SMD	3,7
EO	4
FD	4,3
BD	4,3
WMS	4,7
Do the IMPETUS platform/tools facilitate the cooperation between different actors?	3,9
Is the represented scenario useful to validate the IMPETUS platform/tools?	3,5

The feedback is varied, but in general positive. However, one outlier is the question about whether the operator is overwhelmed by too much information from IMPETUS. This question is scored opposite of all other questions where a lower score is positive and higher score is negative. This is the only question where the score is average. The written feedback in general says that the platform assisted the operator well, but some feedback indicates that there are some need to improve presentation and configuration of tools.

An interesting finding is around the question if the scenario were useful to validate the IMPETUS platform and tools. It was the question that produced the highest separation between the respondents, with not a single respondent answering "3- average". Some of the low scores is connected to expectations to the scenario that is not feasible to play out, but others are probably connected to that the exercise focus on urban security operations may have provided difficulty with showing some tools properly.

From the feedback, the recurring points provided was:

- They found it difficult to observe the screens as there were too few screens for the area and amount of people

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.

- There were some technical issues with loss of connection during the presentations
- It was hard to understand how the environment was inside the SOC as there were no cameras or commentary from inside the SOC

3.2.9 Oslo Live Exercise: Lessons identified and synergies

The live exercise provided opportunity to validate technologies and also identify improvements before the last live exercise of the project in Padova.

The evaluation process was difficult for the evaluators. Several of the evaluation points in the evaluation instrument were hard to observe in a live context and would need improvements before the Padova live exercise. In addition to revising the evaluator instrument, it was also needed that before the next evaluation that the evaluators were prepared better – that they know and understand what systems and operator behaviours are to be expected during the live exercise.

The implementation of an urban security operation focused exercise would not sufficiently show the strengths of all the tools for observers. This would need to be improved before the Padova exercise.

The level of stress within the SOC was successfully generated to be quite high and intense, but it was difficult to observe from the outside of the SOC. Several observers could observe from the activities on the screen and outside and conclude that it must have been quite stressful while others were uncertain of how the environment in the SOC was.

The SMD tool was not showcased properly as there were some problems with access for the KOSS SOC. The report for the analyst was therefore consumed directly by the operator and it made it difficult to assess the impact of the tool

The CTI and CTDR were not optimally showcased in the live exercise. The cyber-attack part of the scenario was the “day before” and did not get played out in a live setting. This reduced the observable utilization of the tools, which would need to be addressed in the next live exercise.

The FD did not respond to the weapon in the crowd, but rather gave an alarm on the holstered weapon of a police officer. The FD had proven to function as intended in both the acceptance pilot and intermediate testing. However, the procedure was still tested and alert sharing to security personnel, which was successful. It is probable that despite training the AI with several datasets in various conditions it would have performed as intended with more training, in particular from crowded scenarios as this.

The UAD alerts were highly sensitive. The sensitivity of the tool will need more work to configure, but it is important to point out that the tool functioned as intended and alerted the operator about the traffic congestion that was synthesised in the dataset. This is a tool that the security organisation will need more experience working with to be able to configure precisely.

The WMS functioned as intended, however the operator noted that the tool could be a source of stress if monitored by himself and have more value if monitored by a supervisor.

The EO functioned as intended and provided the operator a good overview of potential hazards in an evacuation scenario, however it could have been utilized in a better degree with procedures for the various scenarios created.

The BD achieved its test goals, provided the operator with clear oversight of risks, and enabled the operator to alert the Fire and rescue service to handle and decontaminate the affected area and people.

The platform functioned properly and as other tools identified opportunities for technical improvements. Loading times of certain dashboards, real time alert updates and responsive UI for various resolutions and screen sizes.

The communication in the platform however is not a substitute for existing communication technologies. There is potential to integrate this better if the platform is integrated into the normal workflows. The effect of the platforms communication options not being integrated to procedures were visible in the live exercise to the evaluators.

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.

The TRiO system deployed in the Oslo configuration of IMPETUS identified that there is a need between actors that can be fulfilled with a written two-way communication form. The City Hall SOC collected relevant operational information from other actors, such as the evacuation bus was ordered and where it would park. They also provided relevant information to others, such as informing of the threat and various activities, thereby provided nearby SOCs the means to put their own security measures in effect. In example, the harbour authorities just south of the City Hall implemented extra security sweeps of their installations based on this information.

The sharing of the threat information from the IMPETUS platform and the operational overview from TRiO also gave a holistic and accurate situational awareness for the City Hall SOC, as with other actors connected to TRiO. TRiO provided a map view of all the resources connected to the event and map plotting of the event, with relevant locations and functions of the actors involved. The operator had a better understanding of what was happening where and could adjust response accordingly. Such as providing safe passage to the evacuation area in cooperation with other actors involved.

The City of Oslo's perceive that usage of the platform led to several benefits. The playback of the data from the exercise in TRiO indicates that some measures were implemented because of heightened situational awareness and some were implemented faster than expected because of these actions.

It was also successful in addressing new challenges based on new capabilities. In particular after the evacuation when the bacteria detection alerted. This would have had a significant effect in a real incident if the technology was implemented. This triggered questions with several of the external observers that would be affected by such technology about what procedures and handling would be needed in various types of incidents from this capability.

3.3 Takeaways from Oslo to Padova

Outcomes form Oslo Live Exercise have been carefully analysed on several occasions before the Live Exercise in Padova. The first part of this analysis involved the two cities in understanding what worked and what could be improved in terms of general organizations and meaningfulness of the tests.

The Consortium, after some online review meetings, decided that a face-to-face meeting was needed to work together with the aim to boost the technical improvements: the analysis has been hence completed during the so-called bridge meeting in Milano.

An extensive summary of what worked, what were the improvement areas and what has been undertaken during last planning activities, has been attached (see Appendix A). Here below some of the main points addressed.

1. Even if the event has been planned to involve different stakeholders, the end users had to be considered the main target and they deserved maximum focus.

   The output has been: an improved UI and a customized dashboard per kind of end user (they dealt only with the information and alarms that really matter for their own job)

2. From the feedback analysis raised the need to pay more attention to cybersecurity tools and ethics topics

   The output has been:

   - dedicated time and specific end users' involvement for cybersecurity and intelligence tools
   - Live Ex split in 2 days
   - simpler scenario for SOC operators and people in the square
   - involvement of organizations representing citizens, questionnaire and discussion about the ethics aspects

3. External stakeholders, not completely aware of all the undertaken activities, decisions taken, strategies behind, and objectives to achieve, would have liked more info.

   The output has been:

   - audience in front of four screen during the live exercise providing: i. live streaming from the square ii. live streaming from the SOC iii. live reporting from the SOC (short messages

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.

describing what was happening shared via telegram) iv. a presentation supporting the narration of what was taking place

- the exhibition took place in one unique room, before the scenario's sequence of event to let a wider comprehension of the tools
- ten 45-minute webinars (one per tool + PG + platform) undertaken to let the external stakeholder to meet the tech partner and know better the tools' potential
- the appreciated debrief session, with the possibility to interview the end users and collect their direct feedback and feelings, has been repeated

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.

3.4 Padova Live Exercise

3.4.1 Facilitation in Padova

During the Live Exercise in Padova, several locations have been used because of the complex scenario and because several people from different municipality sectors and Police forces have been involved.
Piazza dei Signori: this central square, the sitting room of the city, has been the "theatre" of the outdoor events planned in the scenario.

Nassiriya Room: really close to Piazza dei Signori, this room has been the Consortium Head Quarter

Local Police has been the main stakeholder and several activities took place in their offices:

- ***Office "Polizia Giudiziaria", Via Liberi***: this place hosted the test session related to intelligence activities undertaken by the analysts "the day before"
- ***SOC and HQ, via Gozzi***: the SOC operators, directly using their daily workstations, took their countermeasures agaist what was occurring in the square getting inputs, alerts and additional information from the IMPETUS platform.
- ***Office "Polizia di Prossimità", Prato della Valle*** : here the Consortium involved the external stakeholders showing what happened "the day before", what was occurring in the square and in the SOC. Here also the introduction and the interactive session with the audience, before and after the sequence of the scenario's events, took place.

IT Department – HQ, via Sarpi: as the intelligence analysts and the SOC operators, also the it specialist experts were asked to use the cybersecurity tools directly in their own workstations.

Even if not directly involved in the project developments, National Police and Carabinieri (the national Police forces), as COSSEC members, attended the live exercise in their own SOCs (***National Police local SOC and Carabinieri local SOC***), both connected with the Local Police SOC via the IMPETUS platform, supporting the operations undertaken

3.4.2 How the Live exercise played out

The event started with an explanation about what has been undertaken the day before, when the end users involved have been the IT specialists (**Error! Reference source not found.**) and the Intelligence analysts (Figure 9):

day 1 "Yesterday"- Intelligence and cyber operations prior to the event

- IT specialists interacting with cybersecurity tools (integrated in the IMPETUS platform)
- IT specialists share the threats detected to SOC operators via IMPETUS platform's chat

See

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.

Table 6.

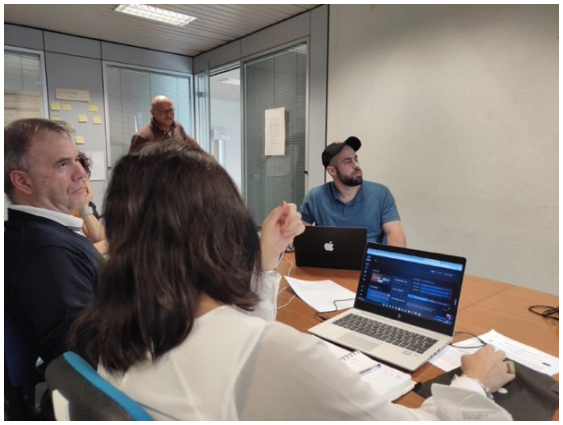
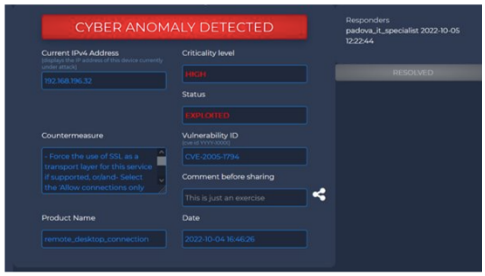
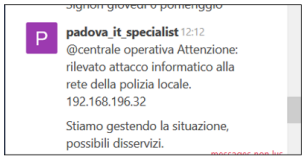


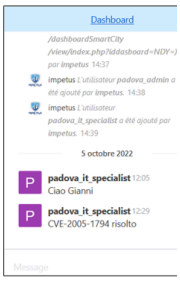
Figure 8 - IT specialists dealing with cyber threats

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.

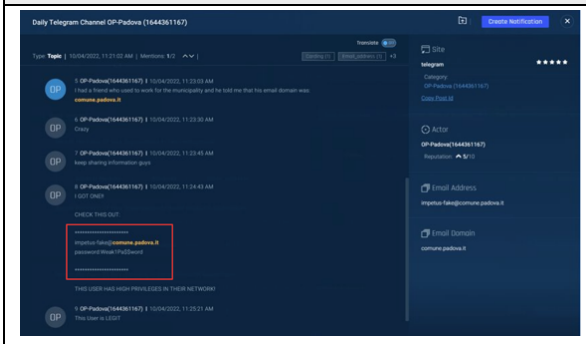
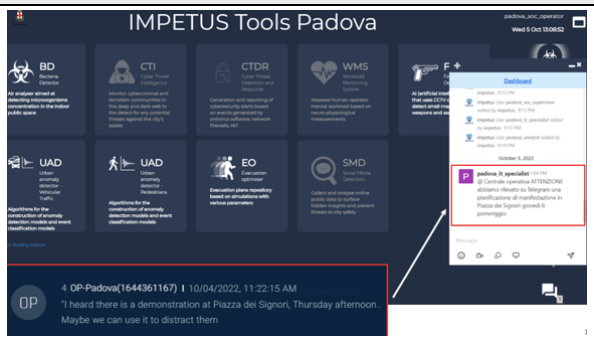
Table 6 – IT Specialists

<table>
<tr><th colspan="2">What (“Yesterday” day 1 - tool CTDR)</th></tr>
<tr><td colspan="2">IT specialists respond to
an attack on the city network

Cyber Threat Detection and Response
Detects cyber vulnerabilities in IT Systems:
raises alerts and suggests countermeasures if they arise</td></tr>
<tr><th colspan="2">How the tool worked</th></tr>
<tr><td>CTDR sends an alert to the IMPETUS platform about the exploited vulnerability and its countermeasures.
 
</td><td>The IT specialist sends a message to the SOC operator about the attack after changing the status of the alert to resolved.
 

Message to SOC operator
 

Message to IT specialist</td></tr>
<tr><td>alerts in the platform</td><td>communication in the platform</td></tr>
<tr><th colspan="2">What (“Yesterday” day 1 - tool CTI)</th></tr>
<tr><td colspan="2">IT specialists detect cyber threats

Cyber Threat Intelligence
Detects, classifies and helps mitigate cyberspace threats to an organisation’s IT assets</td></tr>
<tr><th colspan="2">How the tool worked</th></tr>
<tr><td>  </td><td> 
</td></tr>
<tr><td>Credentials are revealed on Telegram channel</td><td>Communication in the platform</td></tr>
</table>

- Local Police Intelligence Analysts interacting with SMD tool

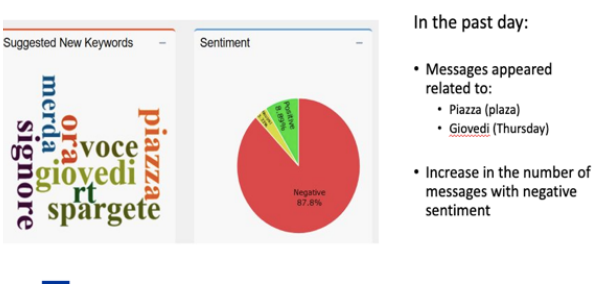
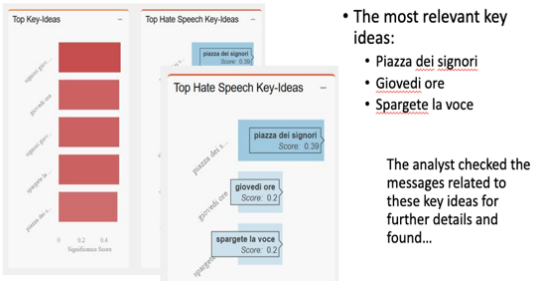
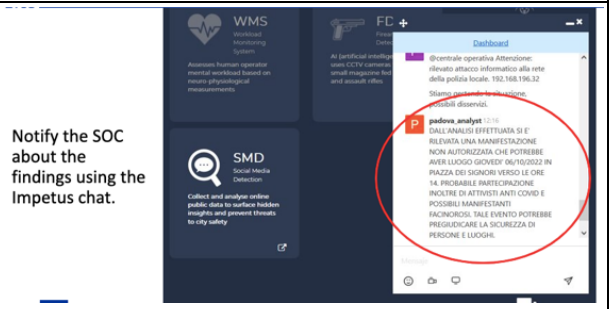
The research leading to these results has received funding from Horizon 2020, the European Union's Framework Programme for Research and Innovation (H2020) under grant agreement n°883286.

Local Police Intelligence Analysts share the results with SOC operators via IMPETUS platform's chat.See Table 7.

Figure 9 - Intelligence analysts searching social media

Table 7 - Intelligence Analysts

<table>
<tr><th colspan="2">What ("Yesterday" day 1 - tool SMD)</th></tr>
<tr><td colspan="2">Intelligence analysts detect threats in social media

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</td></tr>
<tr><th colspan="2">How the tool worked</th></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>SMD dashboard of the analysis</td><td>SMD Keywords and sentiment</td></tr>
<tr><td> 
</td><td> 
</td></tr>
<tr><td>SMD Key ideas</td><td>SMD Sharing findings</td></tr>
</table>

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.

Then, the live event took place. The SOC operators received the warnings about what were discovered form other end users reading the message in the chat and started reacting accordingly (Figure 10).

Figure 10 - SOC Operators react to the inputs coming from the chat

The situation in the square become more complicated (Figure 11 and Figure 12) .

Figure 11 - Many people suddenly entered the square

Figure 12 - demonstration becoming more chaotic, tension raising

With the contribution of the IMPETUS tool the SOC operators were able to solve the potentially dangerous issues (Figure 13).

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.

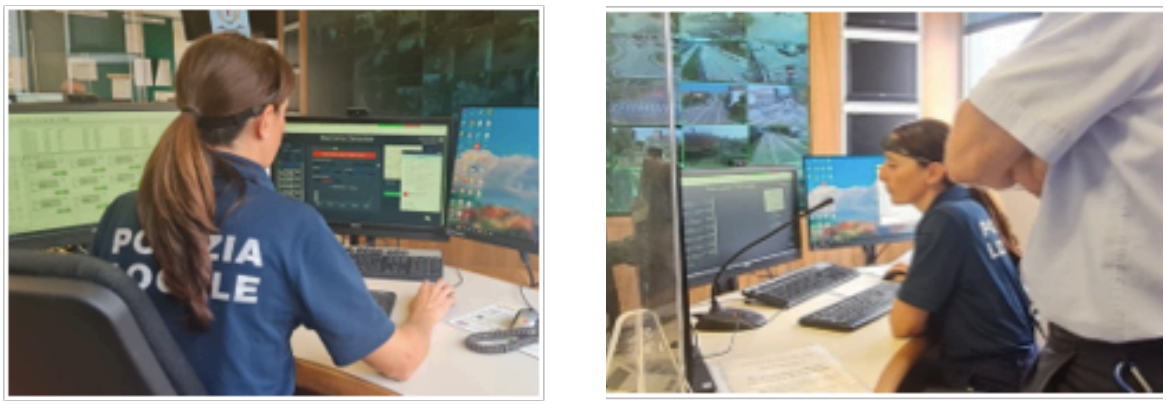


Figure 13 - SOC Operator using IMPETUS

day 2 "Live event" - Real-time operations in Piazza dei Signori

- Overview of the scenario, see Figure 14

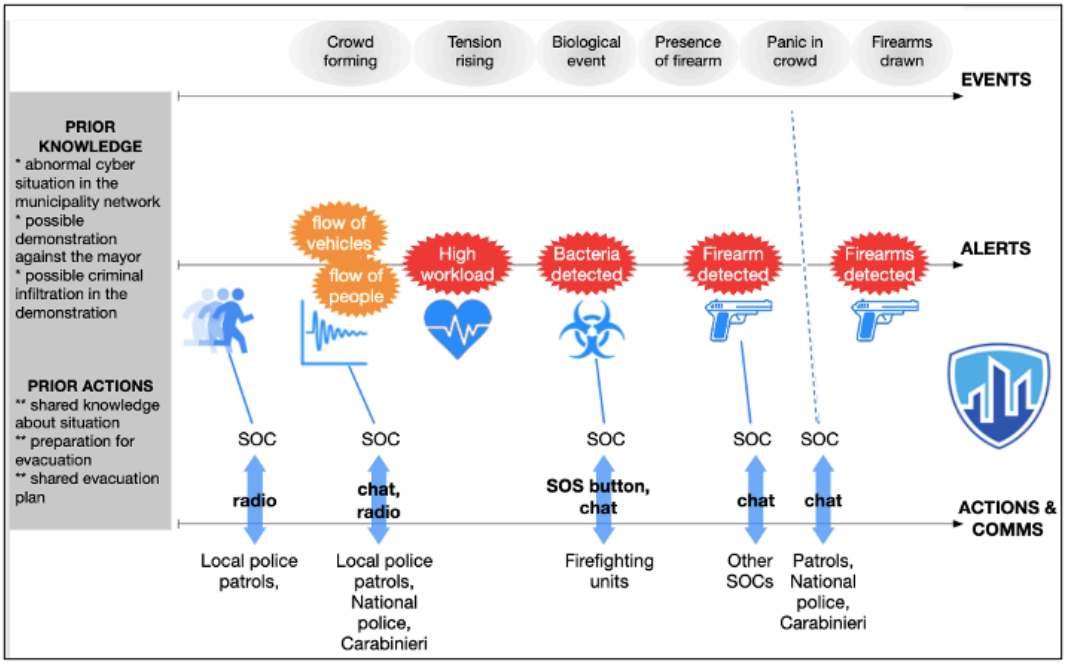


Figure 14 - What happened - sequence of events

- Tools used, see Figure 15.

• Evacuation planning	**Evacuation Optimiser**	Provides instant advice to emergency staff on how to effectively manage an evacuation, based on simulations of different evacuation scenarios
• Unexpected crowd gathering	**Urban Anomaly Detector**	Continuously monitors data gathered from multiple city sensors and detects cases deviating from the norm - possible cause for concern
• Risk to operator workload	**Workload Monitoring System**	Measures mental workload and stress of emergency operators using a brain-computer interface, raises alerts if anomalies arise
• Bacterial event	**Bacteria Detector**	Continuously monitors air samples to detect abnormally high concentrations of airborne bacteria
• Firearm event	**Firearm Detector**	Continuously monitors surveillance camera feeds and automatically creates an alert if a firearm is detected in a public space

Figure 15 - List of the tool used by the SOC Operators

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.

3.4.3 Setting

The locations of the evaluation were provided by the City of Padova. With the aim to evaluate the solutions involving the potential real end users in their own real work environment, the solution related to the cybersecurity were evaluated in the IT department using the end users' workstations during day 1.

The SMD tool have been evaluated during day 1 in the office of the Local Police deputed to investigation activities. While the other solutions have been evaluated in the SOC of the Local Police (based in the Local Police Headquarter), during day 2: two of the four available workstations have been updated to let the SOC operators to interact with the tools –via the platform- in the smoothest way.

The same setting has been undertaken also for National Police and Carabinieri SOC operators (COSSEC members) to let them to simulate a coordinated intervention during the scenario's sequence of events.

3.4.4 Study Participants

With the will to consider different points of view and to enrich the valuable feedback already collected in Oslo, during Live Exercises in Padova other kind of end users have been involved:

- **IT specialists**: a team of 2 expert senior technicians (skilled in networks building and maintaining, bugs detection, and counter cyber-attack actions), Both Italian, 1 female and 1 male.
- **IT supervisor**: Head of the IT dept., decision maker. Italian, male.

  This group of people has been considered representative of IT teams, not only belonging to public administration departments, but also to SME and other kind of organizations (excluding cybersecurity providers that have of course a deeper and wider comprehension of the topic).

- **Investigation Analysts**: a team of 4 people (3 analysts + their supervisor that acted as a specialist), experienced detectives within the Local Police scope/rules of engagement. All Italian, 1 female, 3 males.

  This group of people, even if not perfectly balanced in terms of gender, has been considered representative of those professionals that, within Police forces or other kind of government institutions, have the need to understand what the common sentiment related to a specific event or time is.

- **SOC Operators**: 2 expert members of the Local Police SOC operators' team (~30 people, working in shifts, 4 per shift). Italian, 1 female, 1 male.

- **SOC supervisor:** experienced manager able to manage the SOC operators' team in several kind of different situations, from "normal" status of the city, to high level of emergencies. Able to report to higher level officials (e.g. the Local Police commander), local politicians and authorities (e.g. City Council members and the Mayor), local journalists and other stakeholders.

  These people can be compared in terms of level of experience, skills and duties to the SOC operator involved in Oslo Live Exercise.

3.4.5 Instruments / Measures

During Live Exercise in Oslo, it soon became clear that evaluating the security of the IMPETUS solutions concerning cyberattacks was impossible: the evaluators were able to see the behaviour of the end user, his interaction with the platform and the tools but they could not see impacts of potential cyberattacks on the solutions, during the sequence of the events of the scenario.

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.

The same difficulties have been faced regarding what was planned to evaluate the solutions in terms of ethics. The only significant observable thing has been that the solutions did not harm the end user and there were no gender implications in using the solutions.

Hence, it has been decided to organise the Live Exercise in a different way to create specific room to deepen these 2 important aspects of the project and focus the evaluation on usability and impact on the operations.

With the aim to make in any case a meaningful and comparable observation, the same form used in Oslo – limited to the 2 areas of interest actually evaluable - has been adopted also in Padova.

Evaluators

As already mentioned, the Live Exercise in Padova has been split in to 2 days, with the aim to have more time to evaluate in a more comprehensive way all the solutions.

To evaluate the tools related to cybersecurity and their impact on the IT specialists' daily work, the selected evaluators have been two Italian University teachers, able to deeply understand and to undertake a significant observation. 1 female (eval. A) and 1 male (eval. B)

The SMD tool has been evaluated during day 1, in a parallel session by a legal expert, Italian, female (eval. C).

During day 2, the solutions designed to be adopted by SOC operators (and supervisors) have been evaluated with the same approach used in Oslo: 3 evaluators, with different background, but related to what they have been asked to observe. They were allowed to enter the SOC and directly watch the end users' behaviour and their interaction with the solutions.

To enforce consistency in the evaluations undertaken in both the pilot cities, the 3 evaluators were:

1. eval. A - the Italian University professor involved in day 1 validation activity, female.
2. eval. D - one of the evaluators acting this role in Oslo, Mexican, female.
3. eval. E - the Norwegian SOC operator that was the end user during the Live Exercise in Oslo, male.

All the evaluators have been trained regarding the object and scope of the evaluation (derived from the Validation Plan, D7.1) and the sequence of events included in the scenario.

Procedure(s)/Intervention.
The evaluation took place on October 5 (day 1) and 6 (day 2), 2022.

During day 1, the evaluation of the cybersecurity solutions (CTI and CTDR) lasted ~4 hours (~2 hours per tool). Involved 3 people of the municipality IT dept, interacting with the IMPETUS solution directly within their own workstations.

Here, some specific exercises aimed to test the tools and to improve the level of training of the end users have been undertaken at the beginning of the two sessions. Finally, a real detection of threats based on non-real data injected on purpose has been completed for both the tools. And according to the scenario, a warning communication aimed to provide info about imminent dangers has been shared through the IMPETUS chat with the SOC operators.

In parallel, during the same day 1, the evaluation of the SMD tool has been undertaken at Local Police Investigation Office. ~4 hours, involved four Analysts interacting with the IMPETUS solution directly within their own workstations.

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.

During the first part of the session, the end users were able to complete some simple real investigation analyses, entering keywords and analysing the results.
Then, as planned, they were able to analyse real results of pre-prepared non-real data and they share a warning message via the impetus chat, according to the scenario.

On October 6, day 2, the evaluation took place at the Local Police SOC. 1 hour, 2 SOC operators involved and 1 supervisor.

As occurred in Oslo, The SOC operators were in their 'normal' environment with other colleagues dealing with the city's issues. They were able to interact with the IMPETUS platform via one of the already installed screens to avoid an additional source of information to deal with.
Also in this occasion, the participants were completely free to utilize the IMPETUS platform, aware that the evaluation was ongoing.
As in Oslo, the participants had been wearing the brain computer interface before and was comfortable with it.

After the Live exercise, all the participants have been invited to discuss their experience during a plenary session.

3.4.6 Padova Live Exercise: Overall conclusion and take-aways from the evaluators

As already mentioned, the evaluators followed the same process undertaken in Oslo.
Same sections for Evaluators conclusions:

- Scenario
- Platform
- Evaluation
- Operational
- Usability
- Overall conclusions

Scenario
According to the feedback collected during and after Oslo Live Exercise, the scenario has been reduced and the related activities have been split in two days. The evaluators have been facilitated in undertaking a more comprehensive evaluation.
The sequence of events planned has been considered meaningful and realistic, even if not realistic in sense of the unlikely number of threads in such limited time elapsed.

Platform
The evaluators have been able to appreciate the fine-tuned platform. The updated names of the tools, for instance, made clearer and easier the interaction with the solutions. Adopting a customised version of the platform instead of the general one, let the end users to focus on those significant for their job alarms and information the platform is able to provide.
The exercise allowed a full usage of the CTI and CTDR tools (cybersecurity tools) and a broader. evaluation of the SMD tool.

Operational
The evaluation related to this topic is summarized in the following tables.
To be consisting with the Evaluation in Oslo, here below, firstly, have been reported notes related to evaluation undertaken within the SOC (day 2). Evaluators' comments related to cybersecurity tools and SMD (validated during day 1) are then reported.

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.

Table 8 Evaluator score Operational framework day 2

Operational framework (SOC day 2) - questions	eval A	eval D	eval E
Does the user have increased situational awareness that supports information analysis? Is information providing the operator operational significant insight or combining sources for new knowledge PP-EVAL-41 PP-EVAL-42	Excellent	Excellent	Excellent
The platform provides conditions for collaboration in procedures and response to the event. Actors can collaborate and develop joint situational awareness to assess and adjust response PP-EVAL-24 PP-EVAL-25	Good	Good	Average
The platform provides conditions to adapt procedures and response to the event. The information provides the soc information that is actionable and/or to assess and adjust ongoing response PP-EVAL-27 PP-EVAL-28 PP-EVAL-29	Very Good	Very Good	Good

Operational framework (SOC day 2) – Evaluators' main feedback:

Table 9 Operational strengths and weaknesses day 2

Strengths	Areas of improvement
The system contributes to improve situational awareness.	most of the communication with the agencies and field actors still happens outside the platform
The users have the possibility to share information and indications to other Agencies	The platform does not help the user enough to prioritise and see new/critical alarms,
In case of the FD tool, it is very useful that a picture of the person holding the weapon is sent, together with the map showing the location.	It is required the user pays a lot of attention to the platform to observe that there is a new/critical alarm.

As mentioned, during Live Exercises in Padova validation activities related to cybersecurity and a wider session related to the SMD have been undertaken. Here below, the summary of the evaluators' notes.

Table 10 Evaluator score Operational framework day 1

Operational framework (cybersecurity + intelligence, day 1) - questions	CTDR		CTI		SMD
	eval A	eval B	eval A	eval B	eval C
Does the user have increased situational awareness that supports information analysis? Is information providing the operator operational significant insight or combining sources for new knowledge PP-EVAL-41 PP-EVAL-42	Good	Average	Excellent	Excellent	Very good
The platform provides conditions for collaboration in procedures and response to the event. Actors can collaborate and develop joint situational awareness to assess and adjust response PP-EVAL-24 PP-EVAL-25	Average	Good	Very good	Good	Very good

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.

Operational framework (cybersecurity + intelligence, day 1) - questions	CTDR		CTI		SMD
	eval A	eval B	eval A	eval B	eval C
The platform provides conditions to adapt procedures and response to the event. The information provides the soc information that is actionable and/or to assess and adjust ongoing response PP-EVAL-27 PP-EVAL-28 PP-EVAL-29	Average	Good	Very good	Excellent	Very good

Operational framework (cybersecurity + intelligence, day 1) – Evaluators' main feedback:

Table 11 Operational strengths and weaknesses day 1

Strengths	Areas of improvement
The IT specialists recognised the potential of the CTDR tool in helping to limit the attack surface of the municipality and to increase situational awareness.	CTDR tool: UI and information provided: • some effort in conveying the tool content could exponentially increase the impact of the tool. • the information brought by the graph section is not simple to understand, while the information in the IMPETUS platform can be enriched with more details
Strengths	**Areas of improvement**
The CTDR and CTI tools and the platform provide the technical procedures for implementing collaboration and respond to events	CTI tool: Sometimes the information was even too much and difficult to process for the operators
The operators were happy and understood the potential of the CTI tool defining it "very powerful and complete": it helps into predicting and detecting in advance possible problems. Without the CTI tool, attacks are generally detected only once they occurred: an attack has annoying consequences	SMD tool: limited integration within the platform
CTI provides operators with additional power to spot potential threats before they are exploited.	Platform chat: it does not allow to easily communicate between different departments and confused the operators
SMD tool provides new information to the end user who could manage better potential dangerous situation and could do better operation of OSINT (Open Source Intelligence).	

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.

Usability

The evaluation related to this topic is summarized in the following tables.

To be consisting with the Evaluation in Oslo, here below, firstly, have been reported notes related to evaluation undertaken within the SOC (day 2). Evaluators' comments related to cybersecurity tools and SMD (validated during day 1) are then reported.

Table 12 Evaluator score Usability day 2

Usability (SOC, day 2) - questions	eval A	eval D	eval E
The user has access to the functions of the platform needed to handle and respond to the scenario **(**how often the user mentions a 'missing function' compared to functions that were used during the scenario. PP-EVAL-01)	Very Good	Very Good	Very Good
The user understands can control system functions efficient, the user can control the flow through the application and the behaviour of the system matches the expectations of the user (if the user is using the appropriate function given the step in the scenario, the flow with the expected minimum amount of clicks and the user does not require a lot of mouse movement or unexpected clicks to select the next function given the scenario. PP-EVAL-02 & PP-EVAL-03)	Good	Good	Very Good
When the user encounters a system error or is using the wrong function the user can recover from this error and regain control of the workflow. (quantified by the number of errors that are made and if the user can recover and continue to control the IMPETUS platform. If no error is observed no rating can be given. PP-EVAL-06)	Not Observed	Not Observed	Not Observed

Usability (SOC, day 2) – Evaluators' main feedback:

Table 13 Usability strengths and weaknesses day 2

Strengths	Areas of improvement
The system is intuitive and easy to understand to the user.	Lack of training
The user generally knew how to access the functions to handle the scenario	Communication via chat vs via radio (needed "human contact")
Strengths	**Areas of improvement**
the operator was able to use all the tools and their inputs to overcome the critical situation	Non completed integration (still the need to use different systems)
Massages automatically generated saved time and provided precise and quick info to patrols in the field	Proposed/noted minor changes related to the UI

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.

As mentioned, during Live Exercises in Padova validation activities related to cybersecurity and a wider session related to the SMD have been undertaken. Here below, the summary of the evaluators' notes.

Table 14 Evaluator score Usability day 1

Usability (cybersecurity + intelligence, day 1) - questions	CTDR		CTI		SMD
	eval A	eval B	eval A	eval B	eval C
The user has access to the functions of the platform needed to handle and respond to the scenario (how often the user mentions a 'missing function' compared to functions that were used during the scenario. PP-EVAL-01)	Average	Good	Very good	Very good	Very good
The user understands can control system functions efficient, the user can control the flow through the application and the behaviour of the system matches the expectations of the user (if the user is using the appropriate function given the step in the scenario, the flow with the expected minimum amount of clicks and the user does not require a lot of mouse movement or unexpected clicks to select the next function given the scenario. PP-EVAL-02 & PP-EVAL-03)	Average	Average	Average	Good	Good
When the user encounters a system error or is using the wrong function the user can recover from this error and regain control of the workflow. (quantified by the number of errors that are made and if the user can recover and continue to control the IMPETUS platform. If no error is observed no rating can be given. PP-EVAL-06)	Average	Good	Good	Good	Not Observed

Usability (cybersecurity + intelligence, day 1) – Evaluators' main feedback:

Table 15 Usability strengths and weaknesses day 1

Strengths	Areas of improvement
The operators were happy with the usability of the CTDR.	Non completed integration: the CTDR tool works on three different steps and with three different interfaces (1. NESSUS scan, 2. Creation of the attack graph from the results of the scanning (in the stand-alone tool) 3. Analysis and mitigation/correction of the found vulnerabilities (the details are given in the Impetus interface of the tool)
overall usability and understanding for CTDR was fair	Proposed/noted minor changes related to the UI (e.g. The process for resolving a CVE was quite static and integrated in the IMPETUS platform, without the possibility to reopen a previously closed one)
Strengths	**Areas of improvement**
The operators were happy with the usability of the CTI defining it "a strong step forward"	CTI tool's login function: it requires a pair of credentials making the login process complex and not fully clear for the end users

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.

Strengths	Areas of improvement
SMD tool is easy to use and to manage. The user interface is clear to understand. The users are able to navigate throw the various sections of the tool in a intuitive way	CTI tool's process for resolving a threat: it is not simple to follow and implement. Difficult for the operators to understand the difference between closing a single event and a composite event.
	Using CTI tool, operators were not fully able to understand the difference between imminent and emerging threats
	For CTRD and CTI: lack of training and/or an expert with more specific skills could use the tools in a more effective way

Overall conclusions

PROs

- The evaluators confirmed that the IMPETUS solutions can definitely be considered useful for the users. They indeed strongly contribute to improve the situation awareness. They also potentially provide additional and more precise information and could speed interventions up.
- They potentially can improve coordination and communication among different agencies and/or departments

CONs

- The IMPETUS solutions need specific additional training, they indeed imply a different approach and some specific technical skills.
- Even if the chat has been implemented to provide a simple additional -not exhaustive- communication channel has to be implemented in a different way: voice communication (currently via radio) is still the preferred communication system and the within the platform something to integrate/complete it has to be developed (e.g. videochat and/or instant messaging system like Telegram or WhatsApp)

3.4.7 Padova Live Exercise: Observations tool partners

All tool partners had dedicated personnel to observe the live exercise and provided their feedback in table 14.

Table 16 Tool partner observations Padova

	Padova Live Ex - observations
IMPETUS Platform	There were no technical issues with the platform. The alerts sent by the tools were received and presented in the UI. Telegram messages were sent successfully. Some observations from this Live Ex: the platform should show feedback to the user in order to confirm his/her actions (for example when sending Telegram messages), implement predefined messages to be sent via chat, fix issues related to responsiveness of the UI.

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.

	Padova Live Ex - observations
Social Media Detection (SMD)	In Padova, a group of expert analysts were given access to the platform the day before the Live Exercise. In this case, the project with the dataset was already created. The users were explained the full use of the tool and they were able to find the relevant information for the scenario as well as create some new projects with real data not related to the scenario to get more acquainted with the tool. The evaluation of the tool was complete since the users were giving feedback in real-time.
Bacteria Detection (BD)	In Padova, the SOC operator received the alert and shared this information with the relevant authorities. The feedback from the SOC operator was also good, the information in the interface was easy to understand and handle.
Urban Anomaly Detector (UAD)	During the Live-EX we perturbed real-time data in order to simulate, coherently with the scenario of the Live-EX, many vehicles entering the Padova downtown and, immediately after, an unexpected flow of pedestrians entering Piazza dei Signori. The system correctly recognized such data as anomalies, raised alerts, and allowed the SOC operators to contact the Local Police and report the situation.
Evacuation Optimizer (EO)	In Padova, the operator(s) could access the EO tool during the Live Ex. It happened at different times according to the actual need to analyse the ongoing picture. The operators, among multiple alarms provided by the platform, interpreted the pre-simulated scenarios. At a particular time, the operator has consulted the supervisor on a specific pre-simulated scenario in order to implement proper actions. The dynamic use of the EO tool, based on pre-simulated scenarios, is part of the intended rationale. The communication of specific rules to the street patrols/personnel was not fully analysed, and it was not fully clear whether such information was implemented to govern the evacuation.
Cyber Threat Detection and Response (CTDR)	The CTDR tool could detected the vulnerability exploited from the attack simulation against the Police department network. The CTDR tool proposed a countermeasure to the exploited vulnerability.
Firearm Detector (FD)	The firearm detector detected one small magazine fed handgun out of three even though the shooter was not engaged in a shooting position. The alert was sent to inform the SOC operator. The SOC operator shared this message with the local law enforcement. It was a good exercise because we understood the limits of the detection capacity of the FD tool in an outdoor environment. The feedback from the SOC operator was good, the information was clear and easy to share. However the SOC operator suggested slight changes to the UX (user Experience) to speed up the alerting process.
Work Management System (WMS)	In Padova a single operator used the WMS in the SOC. Initially we wanted to measure workload with a small team, but this turned out to not be possible, due to some availability issues. The WMS system performed well. The earlier calibration was perceived as more relaxed and the operator got to get used to the system a bit more. During the scenario there was one moment the operator got overloaded (high workload alert was issued) and she confirmed this during the after-action review.

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.

	Padova Live Ex - observations
Cyber Threat Intelligence (CTI)	The CTI tool successfully exposed cyber threats against Padova municipality, email domain, and alerted the users on the different threats that were found.

The same questionnaire used in Oslo has been provided to external and internal observers (see addendum C).

A total of 17 questionnaires were returned, 11 internal and 6 external.

The questionnaire asked the participants to assess a total of 14 questions between the range of "1- not at all" to "5 – very much". There were also the possibility to provide some written feedback, which has been utilized by some participants.

Table 15 below, shows an average of the internal observers.

Table 15 Observer Questionnaires Padova

Question	Internals' mark
Is the IMPETUS platform/tools easy to use for the SOC operators?	4,4
Is the information provided easily understandable?	4,4
Do the IMPETUS platform/tools overload the SOC operators with too much information?	3,2
IMPETUS platform	3,6
UAD	4
CTI	3,5
CTDR	3,5
SMD	3,5
EO	4,1
FD	4,1
BD	4,5
WMS	4,2
Do the IMPETUS platform/tools facilitate the cooperation between different actors?	4,4
Is the represented scenario useful to validate the IMPETUS platform/tools?	4,5

It is interesting to notice the increasing trend, in relation with the marks recorded in Oslo: the observers were almost the same in both the Live Exercises, this means that all of them recognised the significant improvement the Consortium has been able to undertake in a couple of months from one Live Exercise to the other.

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.

Instead, almost all the external attenders preferred to not provide a mark to the tools and the platform. Likely, because of some lack of confidence in providing an evaluation, due to a limited knowledge of the solutions and the impacted operations.

The external participants, in their written comments, provided quite different feedback from the internals' one. Indeed, even if they mostly appreciated the event and the developments done, they were not in a position to understand and to clearly see the value added provided.

This, likely, can be partially explained with their limited knowledge of the implemented technologies and concerning Police operations, but there is also another possible explanation: these people should have attended to a different kind of event, less specific and technical, more informative, e.g. more oriented to deepen the ethics aspects.

3.4.8 Padova Live Exercise: take-aways from the observers and external stakeholders (COSSEC members)

The collected comments and observation are summarised in Table 16.

The reader will notice some incoherent sentence related to same topic. This of course is due to the different level of understanding of what has been undertaken.

Table 17 Summary Internal and external observers

Questions for the Observers	Summary of the Answers
1. What did work well? ***(Think about the exercise itself, the platform interface, the tools, etc.)***	· General ORGANIZATION. · AUDIENCE: high interest, many good questions and feedback, good variety of stakeholders; good interaction, specially for PG team with the questionnaire. · SCENARIO: it was able to evaluate tools and platform; better watch the live from a room with the narrator and the multiscreen. · Platform and tools: they worked well, with no bugs/crashes; all the alerts were sent very quickly to the SOC; alerts easy to see; · UI. · MULTISCREEN was good to get involved and understand what was happening. · EXHIBITION before exercise has been better choice than after to explain the tools, sharing knowledge and getting contacts.
2. What did NOT work well? ***(Think about the exercise itself, the platform interface, the tools, etc.)***	· ALARMS: it was possible to see the alerts but no how they solved them, no way to monitor the police response. · TOOLS: no firearm detection for WP, the CCTVs didn't monitor the position but there was no explanation about that; many positive and negatives detection for WP; WP difficult to understand. · PLATFORM: logout from platform to switch to another tool; a lot of reloading gave the impression it was lagging. · MULTISCREEN: small delays between screen and reality. TELEGRAM CHAT: not used as much as we hoped; not clear if it worked · INVOLVEMENT: hard to feel like something is actually happening (es: during firearm detection the moment of the alert was missed); hard to observe tools and platform from the side and without being part of the situation; difficult to catch up with what was happening on the SOC. · NARRATOR: hard to keep the guests engaged and interested in the live ex with the only use of narrator. · SCENARIO: unclear link between tools and scenario; it was both fast and slow; the story was hard to understand for an external observer; no correspondence between narration and video/chat for some details; actions taken by operators to solve an alert difficult to understand

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.

Questions for the Observers	· Summary of the Answers
3. What has been improved from OSLO LEx? (Think about the exercise itself, the platform interface, the tools, etc.)	· Tools names: now they are more intuitive · CHAT: it is possible Sending messages to the whole group of users. · VARIOUS SCREENS: it is possible to have an overall view on all the scenes. · COMMUNICATION: it is possible to see the transmissions of information between SOC operator et SOC supervisor · LIVE: It was very clear what to watch and what to focus on; more visual support for the scenario storytelling; it was clearer for the visitors what each tool did before the scenario started; easier to follow the scenario from a screen sitting in a room; better communication of what is happening; better day scheduling; it has been good having the exhibition before the LIVE with a better engagement of the guests. · WHAT CAN BE IMPROVED? 1. Management and visualisation of alarms. 2. Possibility to track what was going on in the square. 3. Communication among the different actors.
4. What is missing? *(Think about the exercise itself, the platform interface, the tools, etc.)*	TOOL: • FD a correct gun detection; • BD: impossible to understand the SOC operator's response; a deeper integration of the tools • SMD: the audience was not involved in the "day before" exercise, so, for them understanding the analyses and their outcomes was difficult CHAT: it is clear that instant messaging is not the primary communication tool the operators use to communicate (they are used to have only radio communication). PLATFORM: difficult to understand how the SOC operators address the alerts; unclear the colour changing when an alert has been resolved; it is missing an automatic message sent to the involved operative personnel when the alert status changes; not clear what happens after the operator takes in care the alert; coordination/connections between tools SCENARIO: Clear indications of the ongoing events in the square.
5. Something to be underlined (positive and negative)? (Think about the exercise itself, the platform interface, the tools, etc.)	EMERGED ITEMS: 1. to allocate more time for operators training 2. to show the messages that were sent to the SOC the day before to make sure that there is no communication issues. 3. the behaviour of the armed person resulted weird 4. alerts need a level of importance 5. more time for focus groups and feedback on ethical matters. 6. more time to collect and discuss the end-users' feedback and feelings
6. Are the IMPETUS platform/tools easy to use? Articulate your answer. (Think about the exercise itself, the platform interface, the tools, etc.)	The impression shred among all the observers was that the usage of the IMPETUS solutions could be EASY : a limited set of buttons and a clear organization of the information have made the interaction with the dashboard «smooth» for the operators

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.

Questions for the Observers	Summary of the Answers
7. Do the IMPETUS platform/tools simplify the activity of the end-users (i.e. SOC operators)? Articulate your answer. (Think about the exercise itself, the platform interface, the tools, etc.)	YES for the largest part of the audience
8. Do you have other comments/suggestions?	"RADIO or audible messages to speed up the communication." "EO could be integrated with UAD" "The use of the telegram chat and the platform chat are not clear." "I believe that the IMPETUS platform was just a mean to learn and establish the work processes of the SOC operators and the IT specialists. Having said that, we don't have to stick to using the platform". "Tools and the platform, at the end, worked quite well but their real potential did not emerge clearly". "To improve: coordination and interaction between the tools (how the output of one tool can help or serve as an additional feature/input to another tool); prioritize alerts based on modular setting; platform interface to have different views (access control on different resources of the platform) based on different roles of users." "Would be better to have a view on what can be done after the exercise (or after an event): Where the data is stored? How collected data will be used? How will this exercise (and future events) help to improve the responses in the future?"

From the feedback reported in the table, some counter-considerations:

- there have been limited criticisms or misunderstandings concerning the tools and their usage: this means that, for an external point of view, they worked as expected, as the usage and the outcomes of the tools have been perceived as "obvious". Indeed, this is confirmed by the fact that all of the observers were able to notice the difficulties faced by the FD tool. In addition, no one considered any tool pointless or cause of time-wasting
- It was really complicated to let different kind of stakeholders, the most of them far from the end users interacting with the IMPETUS solutions, to have a complete understanding of what has been undertaken. Indeed, the main reported improvement areas are related to this topic. Asking for a clearer understanding means that, apart from some organizational aspects that could have been addressed in a different way (e.g., planning different events for specific targets of audience), there is a clear interest on the evaluated technologies and their implementation / potential adoption. In addition, the potential adding value has been surely understood by this not homogeneous set of people.

3.4.9 Padova Live Exercise: final considerations

The live exercise in Padova has been the last of several stations of the long journey undertaken to evaluate and validate the technologies implemented by the IMPETUS solutions.

All the stakeholders involved, especially the evaluators and the observers, understood the high potential of the developed solutions:

The tools, integrated within the IMPEUS platform, are able to provide additional information and automatically generated alarms that provide an increased situational awareness and let the end users to

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.

take better and quicker decisions concerning what and how have to be undertaken to respond to an emergency or an urgent dangerous situation. Therefore, they are surely useful for the users.

The validated technologies have also an impact on the end users' current operations: an updated mind-set, a specific training and different procedures have to be developed to let the end users to take the maximum advantage from an eventual adoption of the technologies.

In addition, the deeper the integration with the legacy system will be, the more effective will be the usage of the innovative technologies developed.

Another aspect that raised from the validation activities is the stakeholders' involvement.

There are various types of organisations that can be interested in innovative technologies, such as the IMPETUS solutions. The Live Exercise provided a good arena for helping to understand what kind of impact it may have in their organisations.

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.

4 Conclusion

This deliverable is about the usability of the tools and platform, as well as the operational impact on the performance of security and emergency organisations. The live exercises were developed to provide realistic large-scale exercises and to stress operators and the technologies in operation.

The entire consortium were involved in the evaluation process, where three dedicated evaluators were present in the SOC's and others were observing the exercise. In addition COSSEC members and other security and emergency organisations were invited to observe the exercises and provide feedback.

To exploit the advantages of the approach in the project with using lessons learned from each pilot to the next, a bridge meeting was organised between the live exercises. This would help refine the approach before the Padova Live Exercise and would prove to be impactful after Live Exercise.

Usability of tools and platform

The Oslo exercise would reveal a need to revise the live evaluation tool, and as a result the scoring of usability were mostly of a qualitative nature from the evaluators. The Oslo exercise provided an arena where the operator felt the stress to be intense and high, but still felt assisted by the tools and the platform by delivering information that was impactful to the operational assessments and control.

The evaluators noted several opportunities for improving the information flow to the operator, however described it as overall to support the operator's decision-making. The observers would also score 3.9 out of 5, in ease of use for the SOC operator.

Oslo live exercise would leave the operator, the evaluators and the observers' positive to the usability of the tools and platform.

In Padova, the evaluators used the revised evaluation tool and were able to provide scores. The evaluators would score the usability of the tools in the SOC "Good" and "Very Good", while the cyber security and intelligence tools would score "Average", "Good" and "Very Good". The observers would score 4.4 out of 5, in ease of use for the SOC operators.

The SOC operators, analysts and cyber security operators would all be very positive to the tools and the operational insights they provided.

As in Oslo, operators, evaluators and observers were positive to the usability of the tools and platform.

From the live exercises the most common feedback for improvement are within 4 areas:

- Attention to alerts
- Criticality of alerts
- Training
- Communication

The attention to alerts and the criticality is interwoven. Some alerts would not grab the attention, often related to the number of alerts. This was to some degree expected, as the configuration of some tools would require the cities to become very familiar with the sources chosen. The vast number of interactions with the source data and how they could affect the source data would require a greater effort than possible to dedicate to explore, therefor the sensitivity would be left higher than in a real implementation. However, some UI optimizations was identified to increase the ability to grab the operators' attention.

The criticality of alerts was also something the consortium would focus on. This would assist the operators in an emergency where alerts may be frequent to sift through the most vital alerts first. The implementation of criticality could be done in several ways, in example with basic weight of alerts by type of alert from each tool, the alerts can be contextualized to other alerts or smart functionality to provide interpreted alerts. Though providing criticality can be difficult with different technologies. To avoid negative effect and rather to enhance situational awareness, what alerts are critical in a situation may vary greatly with the different capabilities of the tools.

Training is also something that would be important in the usability of the tools. To implement technologies in daily operations will require procedures and organisations that support them based on

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.

local context. Therefore, all training was performed on a generic basis. However, this is important to the operational concepts of IMPETUS and the impact of IMPETUS on security and emergency operations later in the conclusion.

Communication was also identified as a challenge. This challenge relates to the implementation of the chat in the platform. Operators noted that it was not conducive to enhance communication with officers in the field, as written messages were time consuming in producing and consuming compared to radio. This is true in many situations, though the chat was a concept intended to share information between various actors involved in or affected by incidents.

The experience from the Oslo Live Exercise demonstrated that written medium is benefiting operations. By sharing information between actors, it enables them to implement security measures against cascading consequences and sharing of information to improve information pathways for faster response. This also ties into the operational concepts later.

Operational impact

The operational impact on the performance of the security organisations has been considered in two perspectives; what did the technologies contribute with in operation and how is the security or emergency organisation able to leverage the operational impact for increased performance.

Technologies

The evaluation of the platform and the tools were in general positive when evaluating IMPETUS against the operational framework.

The evaluator notes for Oslo would highlight that the platform did well in supporting the operators' decision-making and that the platform provided a holistic and accurate situational awareness. In Padova all three evaluators in the SOC gave the top score (Excellent) that the operators were provided with operational significant insights or ability to combine information to new knowledge. It also scored generally "Good" to "Very Good" on providing actionable information and/or providing ability to assess and adjust ongoing response. The cyber security and intelligence evaluators would also generally be positive also.

In the Oslo Live Exercise there are indications that implementation of some measures can be attributed to enhanced situational awareness, as well as accelerated implementation of some measures.

The perception in the consortium and from the external participants is that there is evident potential to increase performance in security and emergency organisations by utilizing the technologies in their operations.

IMPETUS concepts

The concepts developed in IMPETUS aim at creating resilient organisations that leverage the capabilities in the technologies by increasing the operators' performance and building organisations capable to support operational procedures. The IMPETUS concepts are available in full in the Practitioners Guides developed in the project.

Training

To leverage improved performances for SOCs the perception, comprehension and projection of situations are vital to their situational awareness and affect their decision-making and the efficacy of actions. Hence, the competency of the operators is vital, and to leverage advanced systems in security operations is dependent on developing the operator as much as the systems they use.

However, training will also be dependent on local context. What type of operation it is, what mandate it has, what regulations apply, how the regulations are designed, and local culture will affect procedures as it defines what room for action the organisation have.

Communication

Both cities experienced that since the platform was not integrated in the existing work processes it would have various effects that would be mitigated if this were a system integrated in the daily operations. The most significant aspect of this was the communication system - the chat functionality in the platform.

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.

The experience from the Oslo Live Exercise demonstrated that written medium is benefiting operations. By sharing information between actors, it enables them to implement security measures against cascading consequences and sharing of information to improve information pathways for faster response.

Summary

The Live Exercise scenarios provided the opportunity to create complex and large-scale live exercises that were successful in providing valuable insights to concepts, weaknesses and strengths. The density of events in the scenarios made the operators feel challenged.

One of the primary challenges of implementing platforms with advanced technologies to support operations is to present the right information at the right time in the right context to the operators, which needs to be addressed by every organization based in their local conditions. However, IMPETUS did show the external stakeholders a significant potential value and impact to their security operations.

Overall, the Live Exercises were successful in their missions of: (a) stressing the potential value and the potential challenges in uncertain conditions of using the platform and tools; and (b) assessing the potential impact on security operations. The platform and the tools provided increased situational awareness and supported decision-making, generally scoring well with evaluators and observers in operational and usability aspects.

In the end, both live exercises provided valuable experience and insights:

- All the tools were judged to be providing valuable capabilities
- Roles and competences for each tool were better understood
- The concepts of IMPETUS address the challenges observed in operation
- The increased situational awareness and operational impact were evident

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.

5 Appendix A: Detailed “Lessons learned” and (unedited) feedback

Note: This Appendix contains “raw” feedback gathered during and after the events, in many cases reflecting opinions of individual project members. We have not carried out any editing to align views, remove criticisms etc.

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.

Event preparation and organisation

Worked well	Challenge	Suggestions for Padova	Actions undertaken
Success in putting together a very complex event, no big issue	• A lot happening in the preparation • Limited commitment and proactive participation from the consortium as a whole • Resulted in last minute plannings for several activities with risk to fail EX: registration of attendees, lunch, dinner, facilities needed etc. • In some situations, it was unclear who was in charge and undertaking decisions. This led to confusion in some situations. This is relevant to the need of having more specific and clear role descriptions.	• Need for proactivity in the preparation, answer to deadlines • Need to take a full week from 03/10 • Present facilities planned/available for all partners and for guests early so partners can address needs if not covered • Make clear descriptions between CPAD and SINTEF on who is the lead on what	• “Bridge meeting” in Milano for a deeper analysis of feedback • Webinars about the solutions for external stakeholders to be prepared with “facilitators” (they have been important for the language gap and to train the tech partner to answer questions from non-technical audience) • Defined task forces to address different possible issues and open points • Shared before Lex “Who Does What” reference document
	• Focus of exercise was SOC and management of event - but felt not connected to what was happening in the SOC from the balcony	• SOC operations more visible for guests than only sharing SOC dashboard	• Audience able to see in different screens: 1. what was happening in the square (demonstration and gun holders) 2. what was happening in the SOC 3. mirror of the SOC operator dashboard (as in Oslo) 4. telegram chat with short messages coming from the ” reporter” within the SOC 5. narrator’s presentation

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
	• Not quite sure about how we did for our own purposes • Not a dissemination nor a show • Not a test, but an evaluation of the platform and tools + share the potential • Validation, not verification	• Focus attention on end-users • Focus on partner tools	• Focus on validation: are we developing the right product? → "Useful for the Users" mantra. • All tools challenged. • Focus on end users, involved: ・6 from Local Police (2 SOC operators + 1 SOC supervisor; ・2 Intelligence Analysts + 1 supervisor) ・3 from municipality IT Dept (2 IT Specialists + 1 supervisor) ・2 from National Police (2 SOC operators ・1 from Carabinieri (SOC operator) ・1 Firefighter to provide indication
	Technical issues		•
• Demonstration was working well, good cooperation with police • Smart move to make IMPETUS exercise as part of larger exercise	Unforeseen constraints for gun detection	Establish clear collaboration with law enforcement. Make sure law enforcement allows someone do draw a gun like real shooters do.	• Proper Municipality Authorities and Police forces references involved. • Only policemen authoirzed to hold guns (shooting trainers played the role of the criminals)
It was good that the part of the live exercise that demonstrated IMPETUS tools was part of a wider exercise of greater scale involving many actors: this added to the overall impact of the event.	It was a perhaps confusing for guests that we said "here ends the IMPETUS exercise" when we stopped using the platform, even though the overall scenario that was continuing to unfold was actually part of the same overall sequence of events.	If any similar set-up is planned (i.e. a wider scenario continuing after the "IMPETUS" part), present it as being part of the same overall scenario/exercise, and just say that the demonstration of IMPETUS tools stops at some point (rather than saying the *scenario* stops).	• Planned a large-scale event in a public square during a "common" day (market, people walking, cars, etc.) but mainly oriented to validation activities with limited parallel exercises (e.g. an evacuation trial for municipality personnel) to limit confusion.

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
EXERCISE/EVENT was a success: well planned, well organized, good logistic, good timing, excellent staff/volunteers involvement, well constructed and realistic story/scenario, perfect team work, good communication	Difficult to observe.	Do things with REAL SIMULATION MARKETING for LEx, platform and tools to improve. To connect LIVE in the square with platform MORE TIME to present PG	• Re-shaped scenario • 2 days of validation activities • Re-shaped exhibition • Webinars about the solutions undertaken during the LEx week • Auditorium with 5 monitors to let the audience to better understand • Specific webinar for the PGs • Questionnaires and dedicated time to discuss ethics

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.

Live event, scenario and use of tools

Worked well	Challenge	Suggestions for Padova	Actions undertaken
Exercise successful, dashboard worked, some tools successfully tested			
Live-EX was realistic Scenario was good and stressed-out end-users, especially SOC at City Hall and police SOC	• The scenario tries to cover many tools • Tool: SMD not used, would have appreciated using the tool • Too much focus on specific tools, others no focus • Cyber security tools not visible enough • Integration of Oslo city TRIO tool in IMPETUS was no focus	• Maybe better separate the live tools from the other tools • Group types of tools in one exercise • Not loose live-ex "approach" if tools are grouped • Scenario should have a natural progress and not be "cutted" into different sections away from a realistic timeline • Finding a good (time) balance for tools in use during a realistic Live-EX • If any Padova city tool is integrated in the IMPETUS platform - Live-EX must have focus on this •	• 2 days of validation activities: 5 Oct SMD, CTI and CTDR 6 Oct live tools (EO, UAD, FD, BD, WMS) • 3 session of "hands on" exercises: 1 for IT specialists 1 for Intelligence Analysts 1 for SOC operators • Shorter scenario but continuous sequence of events • More time dedicated to SMD, CTI and CTDR • EO and SMD not used when alarms have been raised • Integration with counter-people sensors and implemented dedicated UAD User Interface
	Platform: not that much going on		
	• Felt too long from the outside • Scenario tempo feels slow • Some escalation, but was it worst case?	**BEWARE**: from the operator, it felt like extreme escalation, a lot going on	• Shorter scenario with a controlled escalation, but with a final complex situation to be handled (3 guns at the same time, just after bacteria attack)
	Supervisor could have been involved to deal with WMS alerts		• SOC supervisor suggested tasks redistribution after detecting high mental workload level watching his own UI

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
	Some guests suggested that some prioritisation of alerts would be useful, and that some kind of "certainty"/"reliability" metric could be part of that.	If technically feasible: consider including this idea.	• Dedicated UI limited the number of alarms. Even if a discussion about how to set an alarm priority, it was not possible to implement it.
The demonstration was convincing.			
platform/tools: worked well and was clear, it was functionally, helpful for the operator. chat in the platform: useful	• TRIO: it is not part of IMPETUS but it was there and it distracted people • too much information at once • not understandable if you did not know the scenario (it happened to guests) • EO not explained • SOC operator took a lot of time in going to another tool	• internet connection with fibre tools • explanation and description for the guests before the live, to make them able to understand what's going on • scenario overview before the live • push notifications for operators inside the platform • guides/group leader for the guests: they can explain step by step • IT analysis + supervisor to add • humanity/human factor to be considered • the event should make the schedule not the contrary • communication to be improved • risk mitigation to be improved software architecture to be improved • to make clear what every screen was showing • to make the scenario more realistic	• all the suggestions undertaken

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
		• CTDR: a better way to show information • EO: need to be clearer • UAD: too much information • SMD: unclear • configuration settings take a lot of space • mobile optimization information about development of emergency could be useful • different colours for different level of emergency • replace name of the tools with role in the platform • more time to prepare exhibition • more time to present PGs	• all feedback addressed

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.

Presentations and narration

Worked well	Challenge	Suggestions for Padova	Actions undertaken
narration was useful as a support for observations and for keeping audience updated in timeline/story	• information provided was too limited • one narrator is not enough • external thought narrator should have been at the centre of the balcony - visible to all	• play-action, not exact actions at exact time • involve multiple narrators and create smaller groups • narrator/note-taker in SOC: • prepared visuals & bullet points; • hand notes / rolling text [see also notes below under "observation of the live exercise"]. • one narrator inside SOC and one outside for the guest → collaboration should be a good approach • **BEWARE**: many narrators can disturb storytelling or end out in communicating differently	• all the suggestions undertaken • audience in 2 rooms, all people able to listen the narrator • simultaneous translation for people not able to understand English • "reporter" wrting notes from the SOC
	• Platform and narration presentation were not visible enough to observers	• Ensure screens are more central • Provide tablets to observers to consult the tablets and tools	• Available 5 big screens with different information + narrator • the same 5 screen in 2 rooms to allow all the people to see and understand what was going on
	• Trio screen was confusing - people did not understand it was something separate from what narrator was talking about, so became rather confused.	• Need to be clearer about what is presented: if there are multiple screens that people can view independently, label them to indicate what they are showing.	• N/A: TRIO is only Oslo's solution
The "Mentimeter" survey (especially the free-text feedback) was useful for simple opinion gathering, and worked very efficiently.	•	• Do this again – maybe just allow, in one survey, people to answer in English or Italian, as they prefer.	• Done

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
	• Weaknesses with presentation of the scenario: • It was not easy to see what was planned to be happening in parallel – "timeline" was essentially linear. • When on the balcony, people simply had to remember what had been explained to them before, in terms of the bigger picture.	• Present the scenario in a "GANNT chart" style to emphasise what is parallel and what is sequential. • Provide participants with the overall scenario in paper form (distributed at registration) that they can have with them throughout. E.G.: Single A4 sheet with "GANTT" on one side and some explanatory text on the other. •	• GAANT Chart style timelime done • Provided more info about the sequence of events before and during the exercise
	• Problems with the one-pager tool descriptions: • Probably, most had not taken the time to read them. • People did not have the one-pagers easily available on the day. • The tool descriptions included a company logo (in some cases several). This gives a "sales" feel which is not appropriate for a LIVEex, and is in not in line with our stated communications strategy (which states that we either show ALL company logos or none). • In some cases the text was too long. • In some cases, the text under the headings did not actually answer the question.	• Improve the quality/clarity of the one-pagers. • Remove company logos. • Create paper copies of the one-pagers and give to guests on arrival. • Use the one pagers in large print size (A3 or A2) as poster at each stand in exhibition.	• Done • Provided QR-code to connect to the project website were the one-pagers have been uploaded (both ENG and ITA) • provided printed copies of the one-pagers • printed A1-posters related to all the solutions to support the explanation during the exhibition
	• People don't understand abbreviations for tools (or for SOC, KOSS etc).	• Definitely don't use abbreviation for tools. • Maybe used "standard" abbreviations (like SOC), but even then explain them.	• All suggestion undertaken

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
Account given by SOC Operator (Magnus) as intro to Q&A session was very helpful indeed in providing a full view of what had happened during the exercise, and the "stress" level in the SOC. Indeed: it was crucial for providing observers who had mostly only seen the outdoor demonstration a fuller picture of the event.	•	• It would be good to have a similar account (language permitting…) from a SOC operator. • Even better: do away with the need for this, by providing video feed, rolling text [see notes below under "Observation of the live exercise"].	• Done the same: during the debrief session almost all the end users involve were asked to witness about their experience and their feelings
	• There were too few screens available. • Not everyone, including a COSSEC member, had an earpiece. • Audio quality could have been better. • the demonstration took a lot of attention. At any given point it felt like the majority was watching the demonstration instead of the presentation. • People started to talk between themselves. • Recurring and quite disturbing technical problems.	• More screen, better audio, greater distance from potentially disturbing elements, thorough testing of the technical solution.	• All suggestion undertaken
NARRATION: very helpful			

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.

Observation of the live exercise

Worked well	Challenge	Suggestions for Padova	Actions undertaken
	• Gap between perception on the balcony and action in the SOC: action on balcony / platform was too quiet while SOC was hectic	•	• Provided several additional means to let the observers and the other stakeholders to better understand
	• Lack of visibility of operations in SOC	• Possible in Padova to film inside the SOC in real time? Possible to approve fixed camera with specific field of view? Possible to have after the fact video if live not real-time? • Is sound possible? radio, phone, etc. • Possible to have someone providing live "commentary" in form of short sentences describing what is going on – and maybe show these on a separate screen (or as rolling text on bottom of another screen)? Maybe even with automated translation e.g. from Italian to English.	• All suggestion undertaken, apart audio form SOC and from the square: local rules and lows do not permit recording voices
	• Lack of visibility of the fire department response to the bacterial alert. They took multiple actions: turned off ventilation system, instructed staff to use face masks, dealt with casualties, performed cleaning. External guests learned of this only later.	• Make sure that all "action" is somehow shown/narrated/reported in some other way (e.g. messages on screen).	• Done
	• Lack of common operational picture of the whole exercise	• Sketch of where organisations are, what people are doing • Drone providing top view of what is happening?	• Reduced the scope of the exercise, provided additional information and possibility to see what was happening

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
	• Demonstration tends to take attention away; the demonstration is not the most important thing to observe and is even distracting. On the other hand: the "live" feel of the voices and the action added a lot to the feeling of "reality" (but 15 minutes or so of that would been enough).	• Screen showing the demonstration could be enough.	• Done: the demonstration has been played in a city center square (Piazza dei Signori while the audience were hosted in 2 rooms with 5 big screens)
	• Platform and narration presentation were not visible enough to observers • Trio screen was confusing - people were not sure about the link with the narration	• Ensure screens are more central • Provide tablets to observers to consult the tablets and tools • Need to be clearer about what is presented	• All suggestions have been undertaken
	• Overall: hard to understand • Chaotic on the balcony	•	• All suggestions have been undertaken
	• LIMITED VIEW: Difficult to watch the screen and to follow the operator work	• MORE SCREEN (far away from demonstration)	• All suggestions have been undertaken

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.

Exhibition

Worked well	Challenge	Suggestions for Padova	Actions undertaken
The informal / conversational / drop-by format worked well [Aris from our sister project said they had used a much more structured/scheduled approach and it had NOT worked well – too rigid + scheduling problems]	•	•	•
Some felt: there were some very good discussions with questions during the exhibition	•	•	•

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
	• Some felt: Exhibition was a bit disappointing	• (maybe) exhibition before for the tools, after for business [Joe: I agree that the idea of "after for business" was indeed part of the feedback. But I feel strongly that we should NOT use the event as a "sales" event – this is not at all appropriate to what we hope to achieve in a LIVEx, and can even be negative. Also, in accordance with our communications plan, we should NOT have promotional materials at the exhibition or elsewhere that show logos of individual partners – that gives a commercial feel. However, if in the course of informal conversations at the exhibition guests ask questions about plans for how tool will be made available post-project, people should have a clear answer ready. Btu this should only be in response to questions. • all tools in the same room • Posters needed	• Exhibition scheduled before the Live Exercise to let th audience to meet the technical partner and the PGs team and to ask questions in a wider way • All the solutions in the same area • All solutions introduced with: ▪ A1 poster ▪ A large monitor ▪ 1 or 2 facilitator/s
	• The different tables could have indicated better what was presented where.	• Some poster or similar with the tool name.	• Done
	•	• MORE TIME TO PREPARE EXHIBITION	• The exhibition room has been set up 2 days earlier • The tech partners and the assigned facilitators were able to prepare a specific webinar and a rehearsal of the exhibition before the Live Ex week and then finetune it

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.

External guests

Worked well	Challenge	Suggestions for Padova	Actions undertaken
Generally, did a good show for external guests	•	• remember: observation not just for guests, primarily for the partners	• Done
	• COSSEC are external so know little about single tools and platform; also tend to have more operational focus. Risk of them being lost following the presentations and narration	•	• Tried a deeper and wider COSSEC and other external stakeholders with: · a dedicated per-solution WHAT IF webinar before the Live Exercise days · shared a per-solution one-pager before the Live Ex (information pack) and during the Live exercise · reshaped the introduction session · scheduled the Exhibition before the Live Ex to let the audience to interview the tech partners about the solutions and the PGs
	• People coming might be more interested in the processes than in the technology	•	
	• At least one guest apologised that he felt unable to provide meaningful feedback on the interface as he had not been able to see it during the exercise.	• We need to make sure that all external guests are able to view operation of the dashboards.	
	• One guest said that he would like to have seen “the tools themselves, not just the platform” in the demo. The way we have designed things, tools can be “visible” in three different ways: (1) Native interface; (2) Limited “dashboard” interface in the platform; (3) Very simple alert/operational status indicator in platform “sidebar”. It is not surprising that guests might be confused.	• Explain this 3-view strategy to guests.	
	• All people cannot understand all aspects	• Video, cartoon for one or two specific points to convey the most important aspects to non-specialists	• No cartoons were possible to be implemented but several additional occasion to get info were provided

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.

Evaluation

Worked well	Challenge	Suggestions for Padova	Actions undertaken
three evaluators for inter-ranking consistency criteria related to assessment instrument; evaluators prepared the scenario and the expectancies related to platform and operator behaviors; evaluators perform a qualitative assessment	• To clearly share the behaviours expected by Platform (when are alerts generated) and operator (how does the operator handle the alerts). It was observed that Impetus platform/tools is yet another information source that is available for situational awareness and operational crisis management (and is not yet part of the set of operational procedures to handle crises. The added value of the platform/tools is therefore difficult to show and evaluate. • How to make sure that real time information from the platform can be made valuable and paid immidiate attention to.	• If the validation scenario is part of a bigger city exercise make the boundaries clear from the start. • Evaluation needs to separate IMPETUS goals from larger exercises • Objective: create a scenario through which the added value of Impetus platform/tools become visible for stakeholders). • Potentially create similar scenario conditions that can be tested with and without impetus. • Include the quantitative loggings from the platform itself in the evaluation report (e.g., time it took the operator after alert on-set to open it, duration of handling, etc). • Added value of the tool in certain type of context can there be different tests • Evaluators spent time together the day before to go through and discuss the scenario in detail and make notes on when to expect the operator to use/intervene with the platform. Highly recommended for Padova	•
presence of native speaker in soc	• Language is key for evaluators	•	•

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.

Worked well	Challenge	Suggestions for Padova	Actions undertaken
platform and tools easy to use and to understand in general the impetus platform/tools simplify the activity of the end-users.	• Easy but too many alarms in a period	• UI/UX, CHAT, ALERTS needs more work to improve	•

"

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.

Demonstration" of ethics work

Worked well	Challenge	Suggestions for Padova	Actions undertaken
"Practitioners Guide" demo at exhibition partially addressed this			
	• One guest pointed out that, while we claim to emphasise work on ethics/privacy, this was not apparent in what we showed.	• The guest suggested inviting some citizen rights group or similar to take part, and provide active feedback/stimulate discussion.	•

Aftermath

Worked well	Challenge	Suggestions for Padova	Actions undertaken
	• Feedback document was complicated to fill for some tools		
	• Real feedback is needed	• direct/open discussion with external guests (e.g., Oslo guests and COSSEC members)	•
	• Lack of presence on social media	•	•

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. What did work well? ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**2. What did NOT work well?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**3. What can be improved for the future?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**4. What is missing?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***
Laurentiu Dragomir (SIMAVI)	· Very well organised. · I noticed a high interest from the guests · The platform and the tools worked very well · The scenario was good	· We could see the alarms, but we didn't see how they were solved	· The tools names are more intuitive · Sending messages to the whole group of users	· Firearm detector – Didn't detect the guns in the crowd and waving guns. The algorithm has to be improved
Simon Hudd (CINEDIT)	· The ability for the observers to engage with the exercise was excellent – the multi-screen setup, the telegram channel, real time view of Piazza dei Signori and the SOC made it easy to feel involved in how many anomalies were addressed. · The process bar made for a very useful visual aid for those watching the exercise, all logistics (compere, translation, Q&A etc) were incredibly professionally managed. · Engagement and interaction from attendees was consistently strong throughout the day, with excellent questions, advice and feedback from an impressive variety of stakeholders and interested parties.	· It was difficult to project the 'expected' stress levels that would have been felt both in Piazza dei Signori and the SOC. · It would also have been useful to have a way to monitor the police response with a visual tool, but these are minor criticisms only.	· I was not present at the Oslo live exercise.	· It was difficult to see and experience how the authorities responded to some of the alerts (i.e. traffic / evacuation) although this was given more context in the spoken feedback session afterwards. I · t also seemed clear that instant messaging is not yet the operational communication tool of choice, and whether there could be a way to build spoken communications into the platform in some way (although the SOC reverted to using radio which may remain the communication of choice for the short term)
Sandrine Bayle	· The observations are easy · Alerts are sent very quickly to the soc for all tools	· Some Firearm aren't not detected during exercise without explanation (no CCTV monitor this position)	· The interface available for the observers · We see the transmissions of information between SOC operator et SOC supervisor	· For biological alert we don't know the SOC operator decision · We don't know if the decision of SOC operator and SOC supervisor is recorded. If the decision is recorded a module can be added in the IMPETUS platform V02 · We don't have the result of the WMS tool
Keren	· The scenario was great for the exercise and it allows evaluating all the tools and the IMPETUS platform.	· Sometimes the end-user has to logout from the platform in order to switch to another tool that the same user should normally be able to have access to the different tools.	· There are various screens. · We can have an overall view on all the scenes. · The volume and internet connection are good.	· Change the colour of an alert when it has been resolved or when it has been identified as a real anomaly. · Also send an automatic message to the rest of the team when the status has changed.

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. What did work well? ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**2. What did NOT work well?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**3. What can be improved for the future?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**4. What is missing?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***
Maria Mirada (iNS)	· The narration of events: putting what we are seeing in a broader context helps massively understand not only the "right now" but also where we are coming from, and potential ramifications /impacts/next steps. · The split screens, different angles/perspectives, chat with logging what is happening… helped get a good feel of everything that was happening. · SIMULTANEOUS TRANSLATION, brava! · Engagement of guests, active with questions and interesting ones at that	· small delays when looking at a screen waiting for something to happen feel much longer and more significant than they are in actual real life. · chat did not load? / wasn't as used as much as we had hoped · UAD - looked like the SOC operator was not understanding exactly what the information she was seeing meant – This is a VERY unsubstantiated observation · a lot of reloading of the platform, gave the impression it was lagging even if it wasn't the case	· I wasn't in Oslo, but I thought the change of the tools names provided more clarity about what it is the tools actually do.	· More intrusive alerts for BRD and FD (imo, their level of severity is not reflected in the current alert system –they are at the same level as bus delays, for instance).
Michelangelo (CINI)	· I would say YES · yes for the exercise overall · yes for the user interface · yes for the tools	· Not clear whether the telegram messaging worked properly	· Much better situation awareness for the observers · It was very clear what to watch and what to focus on	·
Ron (SIG)	· All the logistics around the live ex were amazing and people did an amazing job setting everything up.	· Even though I had the impression that if we will be in a closed room with the screens of all the events around us of the live ex it will be better and easier to understand what is going on, it was still a bit hard to feel like something is actually happening. For example, even the most physical and visual thing which is the firearms detector, I missed the moment of the alert and the moment that it happened in reality. Hence, I think that we should think of evaluating the technology separately from reflecting the events on camera or on the screen. The same way it's hard to show real cyberattack on movies it's hard to show the SOC work on the screen as well. The tools functioned well and as expected but it was just hard to observe it from the side and without being part of the situation. · For an outside observer the events of the live ex weren't happening fast and clear enough. Hence, I am not sure that using a commentator figure for passing along the live exercise events is the right solution. It might be part of the solution but can't be the only one. · Using the commentator makes it very hard to keep the guests engaged and interested in the live ex.	· We had the chance to sit with the IT team and show them the CTI tool and have them use it and take part in the live exercise, unlike in Oslo.	·

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. What did work well? ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**2. What did NOT work well?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**3. What can be improved for the future?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***	**4. What is missing?** ***(Think about the exercise itself, the platform interface, the tools, etc.)***
Thomas (THA)	· Most tools seem to work according to their design.	· Gun had a lot of false positives and negatives. · Link between tools within the scenario was unclear · Scenario was both to fast and to slow · The story of the scenario was hard to understand form the point of an observer	· There was more visual support for the scenario storytelling. · I think it was clearer for the visitors what each tool did before the scenario started.	· Link between tools · A better working dashboard. (Through design and training)
Jelena (ISP)	· Interaction of the externals and the tool operators as well as PG team. · Ethics team collected 50% answers to the survey than expected. Great to have put us all in the same room, and a one with the coffee break table, and to have chairs at our disposal. · Translation.	·	· The organization of monitoring of LEx in a more peaceful environment, with big screen, better focus and clarity and the commentator (Matthieu) was heard more easily.	· I wondered what exactly happens after the SOC operator reacts to the alarm, what are the steps being taken by the police etc. · A bit more story related to the scenario.
Nesrine	· The organisation of the whole Live EX and the scenario setup were good : having the exhibition before the exercise is a good way to show the capabilities of the tools and discuss with guests. · The alerts of different events were coherent and easy to see	· We did not see the chat feature of the platform, but this feature might be not “easy”/non user friendly during a stressful situation. · It was difficult to understand the firearm detection, it seemed the camera did not detect the weapon · It was difficult to catch up with all what was happening on the SOC (the Telegram helped, but we have not explanation on how the issues/events were resolved).	· The organisation of the day is improved, in the sense that we had the opportunity to introduce the tools and discuss with the guests before the exercise (engage them while presenting the different functions, before watching the Exercise) · The communication during the exercise is better: we can see what is happening in different places (square, the SOC, …), we can also see the progress of the scenario in one of the available screens.	· - coordination/connection between the tools (more than including them in the same platform/interface) · We cannot see if there is a link between the results/analysis done the day before and the Live EX events? We cannot understand/see how the pre-analysis (what was presented by Mathieu as the day before scenario) helped to improve responses to the occurred events in the Live Ex
Paolo (UPAD)	· The overall organisation was OK, and the way the exhibition was organised allowed a more effective sharing of knowledge and contacts. · The platform and the functions did not experience bugs/crashes, meaning a stable functioning.	· The execution and dynamics of the scenario were hard to follow. Some details narrated did not correspond to what was provided by the video/chats. · It was hard to understand some passages of the exercise in Piazza dei Signori: the link between the events and the actions taken by operators was not entirely understandable.	· Management and visualisation of alarms. · Possibility to track what was going on in the square. · Communication among the different actors.	· Clear indications of the ongoing events in the square. · Connection between the different tools.

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.

	5. Something to be underlined (positive and negative)? (Think about the exercise itself, the platform interface, the tools, etc.)	6. Are the IMPETUS platform/tools easy to use? Articulate your answer. (Think about the exercise itself, the platform interface, the tools, etc.)	7. Do the IMPETUS platform/tools simplify the activity of the end-users (i.e. SOC operators)? Articulate your answer. (Think about the exercise itself, the platform interface, the tools, etc.)	8. Do you have other comments/suggestions?
Laurentiu Dragomir (SIMAVI)	· No technical problems. The platform and the integrated tools worked very well. · We should allocate more time for training the SOC operators	· Easy and intuitive	· Yes	· Maybe audio message should be a solution to speed up communication between the soc operator and the persons in the field
Simon Hudd (CINEDIT)	· Excellent logistics and organisation across the whole LEX, buy-in from SOC and Stefano's team really shone through. · Excellent attendance for the exhibition, searching questions and interest from attendees. Lots of value for our company in some of the feedback received. · Obvious negative for our tool was the challenge in detecting the weapon, more work clearly to be done in building the model	· From the observer room, it appeared that the SOC operator was able to easily navigate among the tools and to make use of the functionality. As I note above, it did not necessarily show on screen (in real time) to the observers how the SOC reacted to some of the alerts, although this became clearer in the post-LEX feedback.	· Same point as above. It appeared to make SOC's ability to respond easier, although it was not immediately apparent on the screen exactly how they responded to the alerts.	·
Sandrine Bayle	· When the alert is performed, the SOC operator has immediately the information.	· It seems easy as to Sabrina/stephano and Magnus	· I hope I don't know normal situation	·
Keren	· It will be great to show the messages that were sent to the SOC the day before to make sure that there is no communication issues.	· Yes, it seems that the end-users were comfortable using the platform and the tools.	· Yes, the end-user can receive the alerts in the same platform for all the tools.	· EO and UAD could be integrated. So based on the updates of the number of pedestrians and vehicles, the plan of evacuation could be updated. · The synergy and difference between the use of the telegram chat and the platform chat are not clear.
Maria Mirada (iNS)	· the behaviour of the armed person looked very strange · Even though the goal of the live ex scenario was a "stress test", a lot was happening at the same time, so it would have been very hard to follow without the commentary, and sometimes it was even with the commentary.	· It was hard to tell from the screen because we don't know what the users are thinking as they use the tools, but their feedback was quite positive, so yes!	· It does because they have all the alerts in one place and can easily draw connections between the information presented in one (UAD for example and EO)	· JUST RECOGNITION FOR THE AMOUNT OF WORK THAT WENT INTO PREPARING ALL OF THIS LOGISTICALLY, IT IS WAY MORE THAN ONE MIGHT EXPECT.

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.

	5. Something to be underlined (positive and negative)? (Think about the exercise itself, the platform interface, the tools, etc.)	6. Are the IMPETUS platform/tools easy to use? Articulate your answer. (Think about the exercise itself, the platform interface, the tools, etc.)	7. Do the IMPETUS platform/tools simplify the activity of the end-users (i.e. SOC operators)? Articulate your answer. (Think about the exercise itself, the platform interface, the tools, etc.)	8. Do you have other comments/suggestions?
Michelangelo (CINI)	· Very well organized	· The tools require knowledge from the operator. · A training session is necessary to understand how the tools work and how to interpret the results.	· Yes, because it gives the opportunity to the operator to better understand the situation and to communicate with his/her colleagues	·
Ron (SIG)	·	· The platform is pretty simple to use on one hand, but one the other hand I don't think it provide too much of a value on its own.	· My opinion is that for some tools that already have an UI of their own, the IMPETUS platform doesn't add a lot, and in some cases, it might even complicate the work. For the tools that don't has an UI, it's obviously needed.	· I believe that the IMPETUS platform was just a mean to learn and establish the work processes of the SOC operators and the IT specialists. Having said that, we don't have to stick to using the platform. For example, we learned that it's useful to have a chat so the IT specialist can talk to the SOC operators. That lesson can be Implemented in many other ways with many others existent technologies, like Telegram, and not with IMPETUS. · I think other lessons should be pulled out of the IMPETUS platform environment and implemented in a wider perspective that will benefit the users and their day to day work.
Thomas (THA)	· Operator needs better training. · Alerts need a level of importance to support the operator. A bus that is late is probably not as important as a firearm detection. Those important alerts need to be prompted to the user.	· Because each tool has their own interface, that might work well, there is no common interaction design and therefore the whole has a very long learning curve. For example the BRD and FD telegram integration is on gui level complete different.	· Most tools add new information sources that were not available to the user before. · Some tools do help the user. FD can keep track of multiple cameras at the same time. On the video wall you would probably never see a gun as the screens are very small.	·
Jelena (ISP)	·	· I think so.	· I think so.	·

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.

	5. Something to be underlined (positive and negative)? (Think about the exercise itself, the platform interface, the tools, etc.)	**6. Are the IMPETUS platform/tools easy to use? Articulate your answer. (Think about the exercise itself, the platform interface, the tools, etc.)**	**7. Do the IMPETUS platform/tools simplify the activity of the end-users (i.e. SOC operators)? Articulate your answer. (Think about the exercise itself, the platform interface, the tools, etc.)**	**8. Do you have other comments/suggestions?**
Nesrine	· Would love to have more time to be able to set up small focus groups and gather feedbacks on ethical matters from different perspectives	· Seems to be!	·	· Coordination and interaction between the tools: how the output of one tool can help or serve as an additional feature/input to another tool · Prioritize alerts based on modular setting (based on criticity in specific contexts for example) · Platform interface: can we have different views (access control on different resources of the platform) based on different roles of users. · Would be better to have a view on what can be done after the exercise (or after an event): · Where the data are stored? · How collected data will be used? · How this exercise (and future events) will help to improve the responses in the future?
Paolo (UPAD)	· More space for feedback from the end-users · Balanced management of the "Impetus screen" for operators and supervisors.	· It appears ok, but we need to ask the end-users.	· It appears yes, but we need to ask the end-users.	· Some progress from OSL has been done but the potentiality as a whole platform did not emerged so much. · I think it would be better to focus more on the platform rather than the single tool.

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.

	Is the IMPETUS platform/tools easy to use for the SOC operators? (1 = Not at all, 5 = Very much)	Is the information provided easily understandable? (1 = Not at all, 5 = Very much)	Do the IMPETUS platform / tools overload the SOC operators with too much information? (1 = Not at all, 5 = Very much)	Do the IMPETUS platform/tools show the right information? In case, what is missing? (1 = Not at all, 5 = Very much)	Do the IMPETUS platform/tools facilitate the cooperation between different actors? (1 = Not at all, 5 = Very much)	Is the represented scenario useful to validate the IMPETUS platform/tools? (1 = Not at all, 5 = Very much)
Laurentiu Dragomir (SIMAVI)	5	5	2	1,1,1,1,1,2,3,1	5	5
Simon Hudd (CINEDIT)						
Sandrine Bayle	4	4		4,5,5,5,5,5,5,5,5	5	5
Keren	5	5	1	4,5, , , ,5,5,5,5	4	5
Maria Mirada (iNS)	4	4	3	4,3, , , ,5,5,5,5	4	4
Michelangelo (CINI)	4	4	4	5,5,5,5,5,5,5,5,5	5	5
Ron (SIG)						
Thomas (THA)	4	3	4	3,3,3,3,3,3,3,3,3	3	4
Jelena (ISP)	5	5	4	4,5, , , , ,4,5,5	5	5
Nesrine		5	4	3,5, , , ,5,4,5,5		3
Paolo (UPAD)		5	4	, , , , , 2, , , ,		

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.

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.

6 Appendix B: Forms given to evaluators during Live Exercises

Exercise IMPETUS Live Exercise
Location: XX
Date: DD MM YY

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.

Objective 1:
The usability of the IMPETUS Platform

List of criteria to be measured		Observed (O) Not Observed (NO) Not Applicable (NA)	Rating Below Average (BA) Average (A) Good (G) Very Good (VG) Excellent (E)	Overall Rating
1	The user has access to the functions of the platform needed to **handle and respond to the scenario.** This can be quantified by how often the user mentions a 'missing function' compared to functions that were used during the scenario. PP-EVAL-01			
2	The user understands can control system functions efficient, the user can control the flow through the application and the behaviour of the system matches the expectations of the user. This can be quantified by if the user is using the appropriate function given the step in the scenario, the flow with the expected minimum amount of clicks and the user does not require a lot of mouse movement or unexpected clicks to select the next function given the scenario. PP-EVAL-02 & PP-EVAL-03			
3	When the user encounters a system error or is using the wrong function the user can recover from this error and regain control of the workflow This can be quantified by the number of errors that are made and if the user can recover and continue to control the IMPETUS platform. If no error is observed no rating can be given. PP-EVAL-06			

General Comments:

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.

Objective 2:
The applicability of the IMPETUS ethical framework

List of criteria to be measured		Observed (O) Not Observed (NO) Not Applicable (NA)	Rating Below Average (BA) Average (A) Good (G) Very Good (VG) Excellent (E)	Overall Rating
1	**All personal data collected by various IMPETUS Platform Tools are secured and accessed only by authorized personnel (in accordance with GDPR Regulation and LED Directive)** **Is the observable physical security and procedures satisfactory to safeguard the information**			
2	**Does the platform guarantee the "respect of the human autonomy" in every UI?** **Is the end user always able to decide if and when to intervene? is there any critical automatism the end user cannot control? Ref PP-EVAL-17.**			
3	**Does the platform guarantee the "prevention of harm" in every UI?** **Is there the risk to "create" a potential (adding) danger to the end user or to other stakeholders (citizens first)? Is there the risk to have worse situation than the previous one? Ref** **PP-EVAL-18.**			

General Comments:

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.

Objective 3:
The impact of the IMPETUS operational framework

List of criteria to be measured		Observed (O) Not Observed (NO) Not Applicable (NA)	Rating Below Average (BA) Average (A) Good (G) Very Good (VG) Excellent (E)	Overall Rating
1	**Does the user have increased situational awareness that supports information analysis?** **Is information providing the operator operational significant insight or combining sources for new knowledge PP-EVAL-41 PP-EVAL-42**			
2	**The platform provides conditions for collaboration in procedures and response to the event.** **Actors can collaborate and develop joint situational awareness to assess and adjust response** **PP-EVAL-24 PP-EVAL-25**			
3	**The platform provides conditions to adapt procedures and response to the event.** **The information provides the soc information that is actionable and/or to assess and adjust ongoing response** **PP-EVAL-27 PP-EVAL-28 PP-EVAL-29**			

General Comments:

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.

Objective 4:
The effectiveness of the IMPETUS cyber security framework

List of criteria to be measured		Observed (O) Not Observed (NO) Not Applicable (NA)	Rating Below Average (BA) Average (A) Good (G) Very Good (VG) Excellent (E)	Overall Rating
1	Is there evidence of cyber security vulnerabilities If observations are made, please use comments to specify.			
2	Is there evidence of insecure practice If observations are made, please use comments to specify.			

General Comments:

Additional Comments:

Name of Evaluator:

Agency:

Date:

Name of manager or supervisor sighting 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.

7 Appendix C: Feedback questionnaire for internal and external observers

Please indicate your role in your organization:	
Please rate the following criterions based on your opinion (1 = Not at all, 5 = Very much):	
Is the IMPETUS platform/tools easy to use for the SOC operators?	○ ○ ○ ○ ○ 1 2 3 4 5
Is the information provided easily understandable?	○ ○ ○ ○ ○ 1 2 3 4 5
Do the IMPETUS platform/tools overload the SOC operators with too much information?	1 2 3 4 5 ○ ○ ○ ○ ○
Do the IMPETUS platform/tools show the right information? In case, what is missing?	
IMPETUS platform *What is missing (if any):*	○ ○ ○ ○ ○ 1 2 3 4 5
Urban Anomaly detector (UAD) *What is missing (if any):*	○ ○ ○ ○ ○ 1 2 3 4 5
Cyber Threat Intelligence (CTI) *What is missing (if any):*	○ ○ ○ ○ ○ 1 2 3 4 5
Cyber Threat Detection and Response (CTRD) *What is missing (if any):*	○ ○ ○ ○ ○ 1 2 3 4 5
Social Media Detection (SMD) *What is missing:*	○ ○ ○ ○ ○ 1 2 3 4 5
Evacuation Optimizer (EO) *What is missing (if any):*	○ ○ ○ ○ ○ 1 2 3 4 5
Firearm Detection (FD) *What is missing (if any):*	○ ○ ○ ○ ○ 1 2 3 4 5
Bacteria Detector (BD) *What is missing (if any):*	○ ○ ○ ○ ○ 1 2 3 4 5

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.

Workload Monitoring System (WMS) *What is missing (if any):*	○ ○ ○ ○ ○ 1 2 3 4 5
Do the IMPETUS platform/tools facilitate the cooperation between different actors?	○ ○ ○ ○ ○ 1 2 3 4 5
Is the represented scenario useful to validate the IMPETUS platform/tools?	○ ○ ○ ○ ○ 1 2 3 4 5

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.

Members of 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

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.

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
TIEMS	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

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.