IMPETUS

Project results

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 Practitioners 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, legal and data privacy 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) hosted practical trials of the IMPETUS solution during the project lifetime.

The long-term goal is to use these trials as a demonstration of the viability of using advanced technology of the type developed in IMPETUS. This will encourage much wider uptake, not only geographically but also in terms of other technologies that may emerge in future.

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.

Project duration: September 2020 - February 2023.

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

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

IMPETUS Results

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

Practitioners Guides

Bringing the lessons learned
from IMPETUS to a wider audience

WHAT PROBLEM DO THE GUIDES ADDRESS?

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

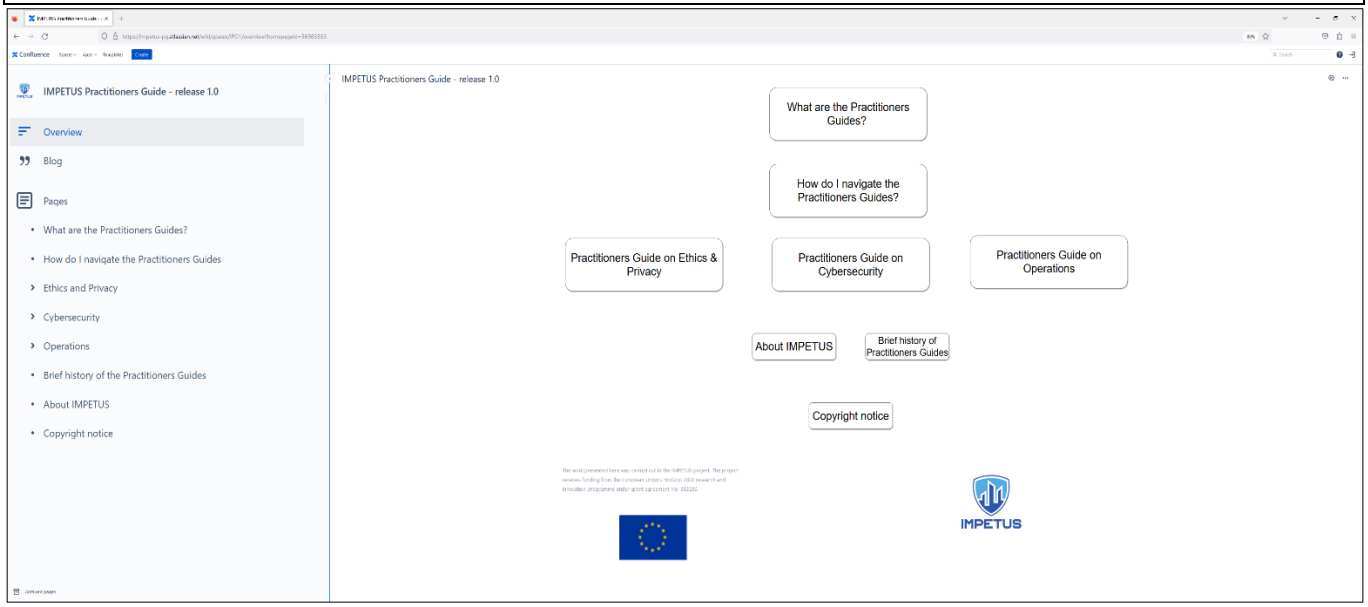
In IMPETUS, we developed approaches to addressing these issues, and learned many valuable lessons along the way. The Practitioners Guides raise awareness and bring lessons learned in IMPETUS to a wider audience. They consist of guidelines, tutorial materials, checklists, reference information and more,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

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

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

HOW ARE THE GUIDES INTENDED TO BE USED?

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



HOW DOES IT WORK?

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

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

Firearm Detector

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

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

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

Without this tool:

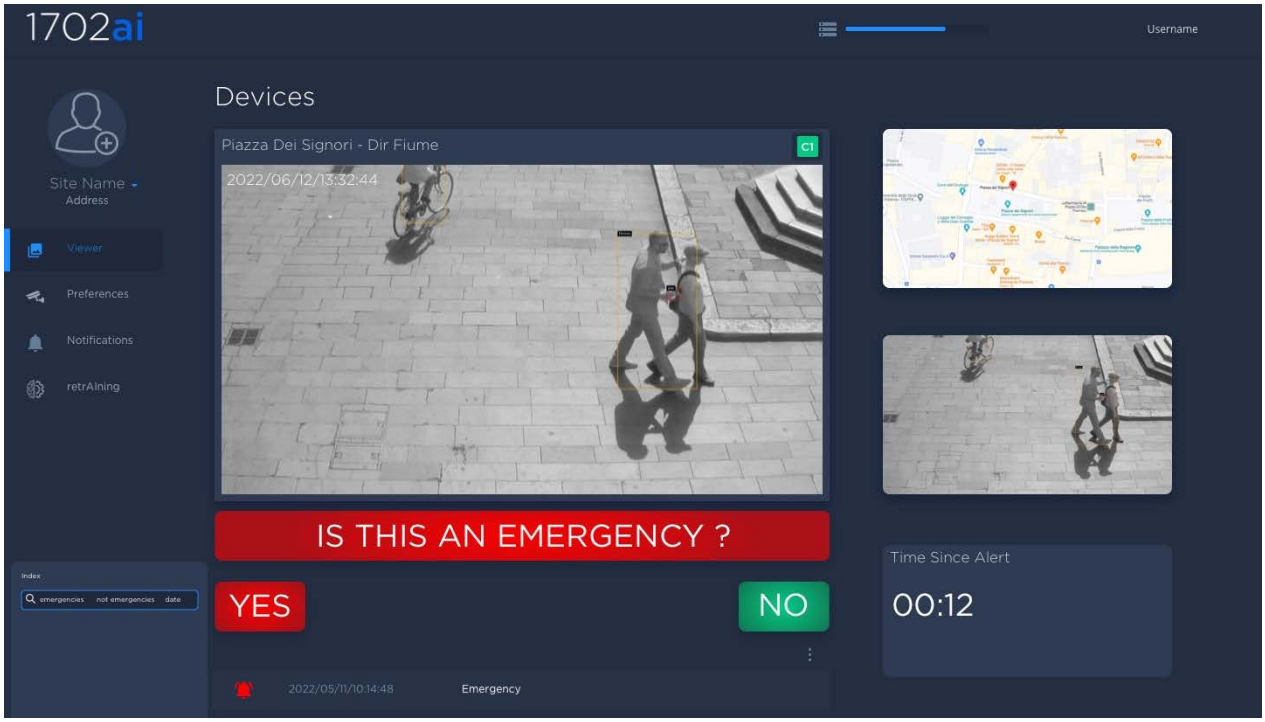
- Law enforcement is hindered due to the lack of detailed situational awareness (delays and uncertainties in reporting, lack of information about exact location)
- Response times can be lengthy – and in situations where every second count, this can lead to loss of life

With this tool:

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

HOW IS IT DEPLOYED IN IMPETUS?

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



HOW DOES IT WORK?

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

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

Bacteria Detector

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

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

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

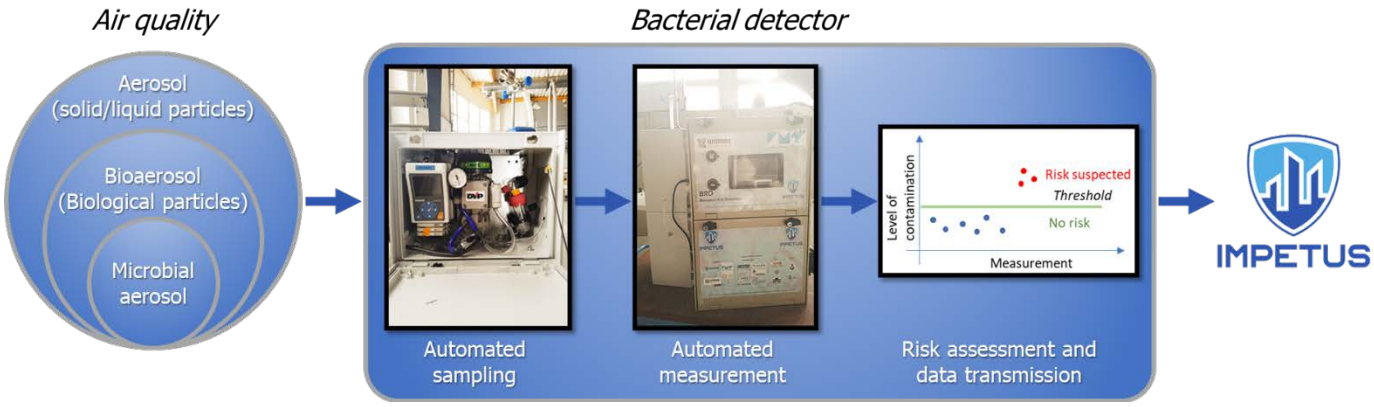
- One person can infect 1–10 other people, depending on the pathogen
- Physicians need to take samples from patients to find a suitable treatment, which prolongs treatment
- Hospital staff are not protected, and an epidemic can be declared the day after the disease appears

With the tool:

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

HOW IS IT DEPLOYED IN IMPETUS?

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



HOW DOES IT WORK?

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

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

Urban anomaly detector

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

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

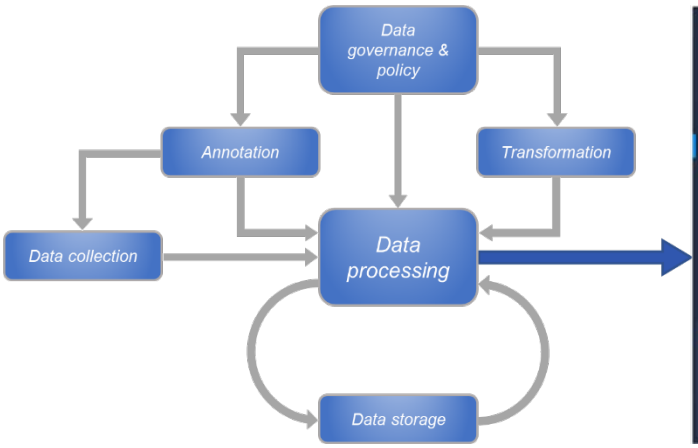
Smart cities continuously gather data from multiple sensors throughout the city. While variations in the data can be a sign of possible problems, the volumes of data are typically so huge that it is not feasible to monitor manually, or easily detect anomalies.

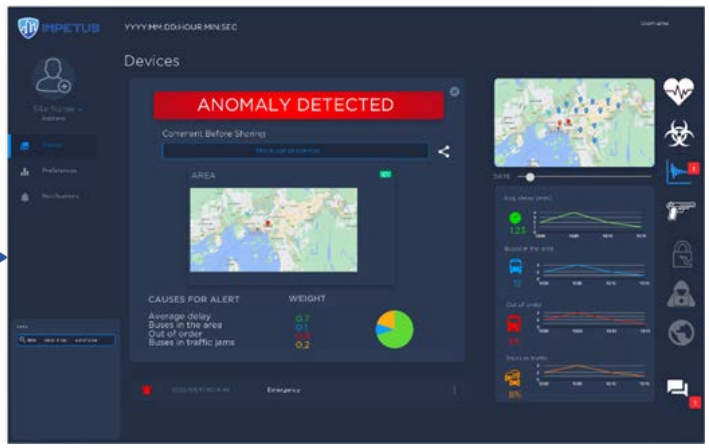
The tool uses AI (Artificial Intelligence) techniques to gather data from multiple sources over long time periods to recognise patterns and recognise what is "normal" at different times and places. It then uses that knowledge to detect anomalies when they occur, even if they have not been observed before. The tool can categorize anomalies and let a human operator evaluate whether they represent a real danger.

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

HOW IS IT DEPLOYED IN IMPETUS?

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





HOW DOES IT WORK?

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

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

Social Media Detection

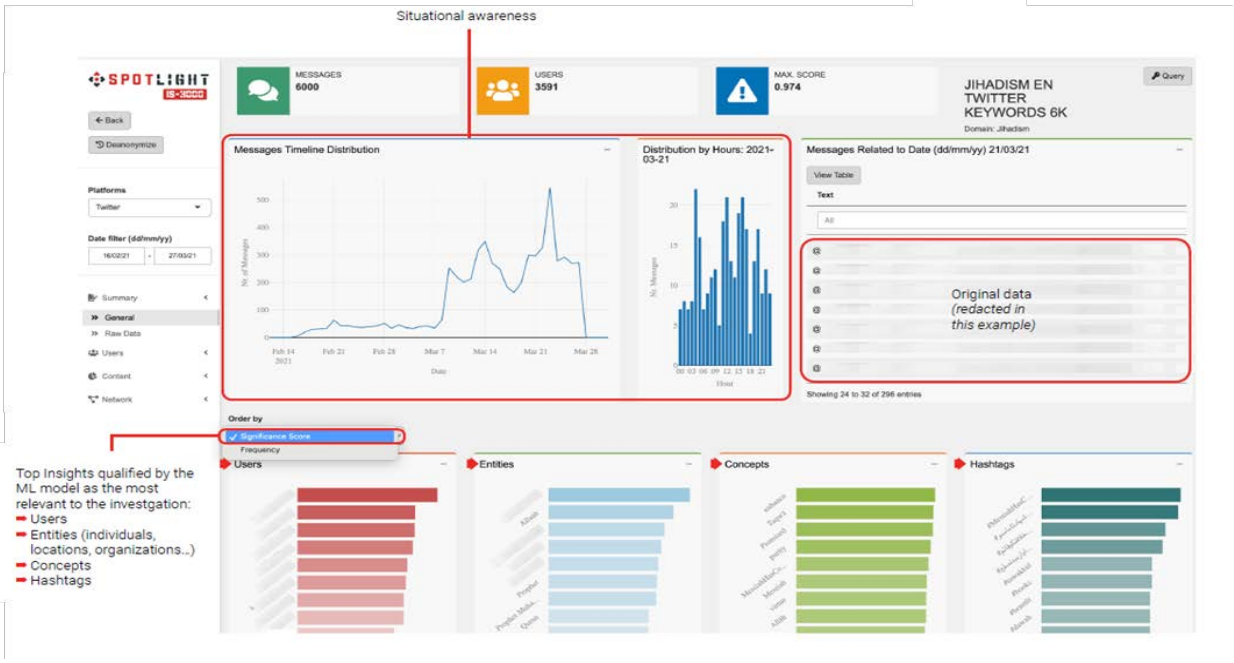
Scans large volumes of text on social media and other public online sites, looking for topics/keywords that might indicate potential trouble or threats

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

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

HOW IS IT DEPLOYED IN IMPETUS?

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



HOW DOES IT WORK?

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

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

Evacuation Optimiser

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

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

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

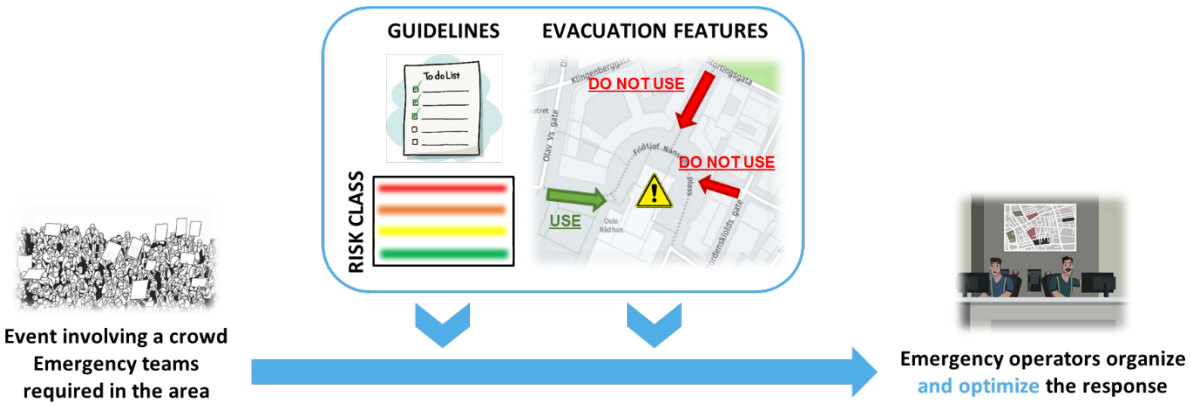
- The adequacy of number and size of exit routes is unidentified
- Specific gateways for emergency services are not known
- The total evacuation time and risk associated with evacuation remain unknown

With the tool:

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

HOW IS IT DEPLOYED IN IMPETUS?

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



HOW DOES IT WORK?

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

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

Cyber Threat Intelligence

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

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

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

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

With the tool, you are able to:

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

HOW IS IT DEPLOYED IN IMPETUS?

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

HOW DOES IT WORK?

There are 3 main steps:

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

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

Cyber threat Detection and Response

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

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

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

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

Without the tool:

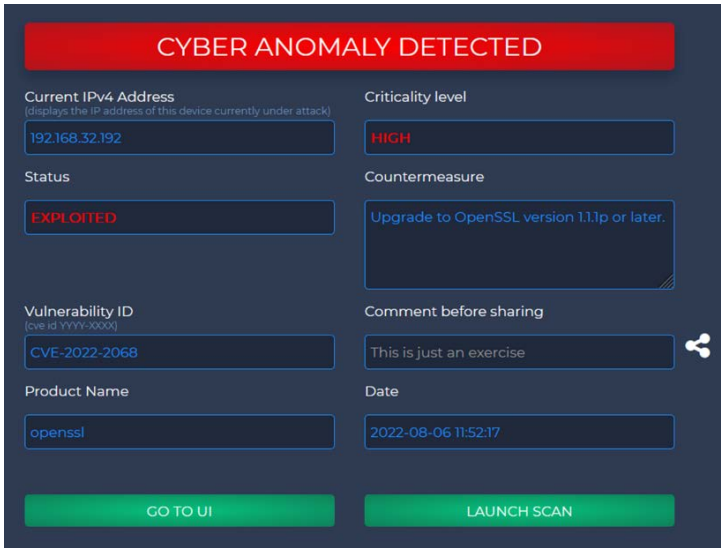
- Users' manual analyses of the system identify only a fraction of the vulnerabilities inherent within the system
- Users are not aware of how inter-linked vulnerabilities could expose the system
- Users are not aware when a vulnerability has been exploited

With the tool:

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

HOW IS IT DEPLOYED IN IMPETUS?

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



HOW DOES IT WORK?

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

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

Workload Monitoring System

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

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

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

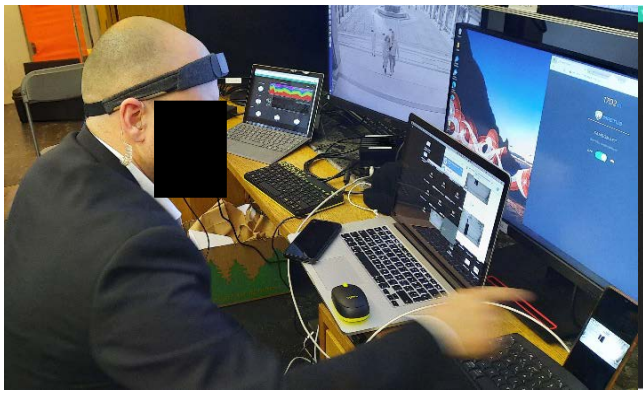
- Workload perception is implicit, subjective and sporadic

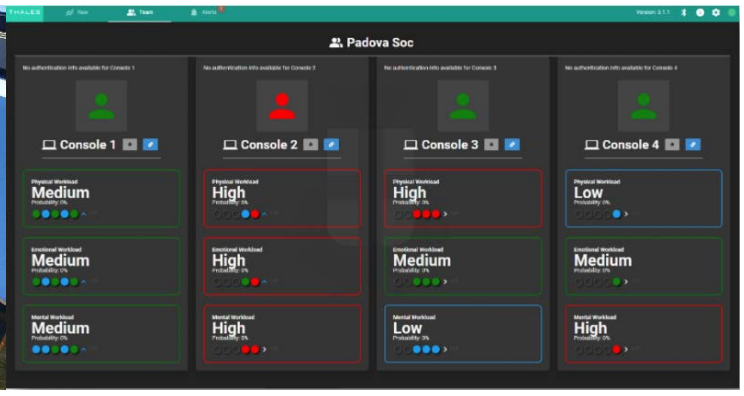
With the tool:

- Workload assessment is explicit, objective and continuous

HOW IS IT DEPLOYED IN IMPETUS?

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





HOW DOES IT WORK?

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

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

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

The IMPETUS Platform

Integrates multiple tools in a unified interface

WHAT PROBLEM DOES THE TOOL HELP SOLVE?

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

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

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

HOW IS IT DEPLOYED IN IMPETUS?

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

HOW DOES IT WORK?

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

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

Results summary

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

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

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

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

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

The IMPETUS Consortium

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

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