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: D4.3

Interface Design and Big Data Visualization

Dissemination Status: Public

Editor: Maria Mirada, INS

Authors: Maria Mirada, Guillem Garcia, Joaquín Luzón, Raul Mendez (INS), Bruno Bonomini, Arianna Dissegna (CPAD), Joachim Levy (CINEDIT), Ian Simon Gjetrang, Magnus Devik Borge (OSL), Matthieu Branlat, Martina Ragosta (SINTEF), Thomas de Groot, Iris Cohen (THA), Keren Saint-Hilaire (IMT), Alexia Comte, Mathieu Tur, Sebastien Courtin (UdN), Ron Ofer (SG), Michelangelo Ceci, Chiara Braghin (CINI), Matteo Bottin (UPAD), Thomas Robertson (TIEMS).

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

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 introduces the User Interface (UI) for the IMPETUS platform. Considering that the end users that will be leveraging IMPETUS in their daily lives have different roles, responsibilities and tasks, the first part of this deliverable focuses on describing the specific requirements for SOC Operators, SOC Supervisor, IT Operators, IT Supervisors, Intelligence Specialists and Technical Administrators, and covering what specific tools are better suited for each specific role.

The design of the UI focused on consistency and modularity as its main guiding principles, ensuring that the look and feel is cohesive across the whole platform while allowing for the possibility of adapting it to the needs of each specific end-user. For instance, having a side bar that does not cover the whole screen was crucial for the SOC Operators, whereas this feature is optional for IT Specialists or Intelligence Specialists.

Along with the sidebar, the chat, the home page, the alerts and the tools dashboards constitute the main components of the UI. It is noteworthy to mention that, in terms of UI development, the tools belong to 2 major groups: those with UIs developed specifically for IMPETUS and those with pre-existing proprietary UIs. For the first ones, the IMPETUS UI constitutes a self-contained visualization platform, where all functionalities are incorporated into the IMPETUS UI. For the latter ones, the goal has been to integrate into IMPETUS those functionalities, mostly in the form of alerts, that provide the most immediate value to the end users, making the IMPETUS interface and the external UIs interact in the most efficient way possible and without redundancies.

This document provides further details about all the points presented above and includes screenshots (static representations of the platform interface) for all the elements described, along with an explanation of the evolution that led the Consortium to the final version.

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.

List of Figures

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 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
UI	User Interface
BRD	Bacterial Risk Detection
CTI	Cyber Threats Intelligence
CTM	Cyber Threats Mapping
HCI	Human Computer Interaction *[1]
PTI	Physical Threat Intelligence
PTRO	Physical Threat Response Optimization
SMD	Social Media Detection
WD	Weapon Detection
CPAD	City of Padova
OSL	City of Oslo
SOC	Security Operations Centre
COSSEC	Community of Safe and Secure Cities

[1] The HCI was renamed Workload Monitoring System (WMS) to make the title more descriptive of the tool functional

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

The primary target audiences for this deliverable are the end users of the tool and their supervisors, followed by Consortium members (particularly tool providers), COSSEC members and other stakeholders interested in the visual representation of the IMPETUS platform.

For end users and supervisors, it is an excellent way to get familiarized with the look and feel and structure of the platform. For tool providers without a previously developed proprietary interface, this deliverable shows how their algorithms and technology have been translated into interfaces the end users can interact with, and tool providers with a previously developed proprietary interface will see how and to what extend their platforms have been integrated/communicate with IMPETUS servers.

For COSSEC members and other stakeholders, this deliverable offers an overview of the steps taken for the creation of the UI (User Interface) and a recompilation of the UI screenshots, which can be interesting from a procedural standpoint, leveraging it as a blueprint or as guidelines for future similar projects or as a foundation on which to expand.

This deliverable can also be of interest for a broad spectrum of researchers and technology developers interested in the decision-making process and strategies applied to interface design, attention management, big data visualization and general sense-making of systems deployed in smart cities operational ecosystems.

1.2 Why would I want to read this deliverable?

This deliverable can be attractive to readers interested in learning about the integration of different tools in the context of for smart cities systems from the perspective of the user experience.

Firstly, this deliverable walks the reader through the thought process and resulting design choices and strategies applied to put forward a user interface that takes into account, works within and attempts to mitigate or address some of the challenges faced by smart cities operators, particularly around attention management mechanisms (capturing the operators' attention), sensemaking enhancement (situational awareness) and streamlined communication.

Secondly, it provides one possible answer to the question about how to combine into one system tools widely diverse in nature, in level of integration and in scope (accuracy and validity of the answer will be validated during live exercises). Thirdly, this deliverable also elaborates on what principles have been followed when approaching big data visualization strategies from the perspective of the end user.

Finally, it offers a guided tour of the whole IMPETUS interface, namely the look and feel of the platform, its transversal sections, the individual dashboards and alerts for each of the tools, besides mapping out the different access pathways to the external proprietary UI of the tools that have them.

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.

1.3 Structure

This document is organized to first provide a description of the different profiles of end users that will benefit from using the IMPETUS platform in their day-to-day work, covering their different needs, responsibilities and how they will interact with the platform as a whole and with each of the tools in particular.

The second section, the most extensive one, introduces the IMPETUS interface, elaborating on the evolution the design has followed from the initial drafts to the final version, it explains the tools' varying levels of integration with the IMPETUS platform and what design guidelines were applied during the development of the UI. Additionally, this section describes the main transversal elements of the UI (Side bar, home page, chat) and presents the UI screenshots for each of the tools grouped by user profile. These UIs have been designed through a collaborative process of informed decision making and already conform an operational interface. However, in light of the validation results and input from stakeholders during the live exercises, it may further evolve to incorporate identified improvements and adjustments.

Finally, it explains how Big Data Visualizations have been approached and briefly sets the stage for potential future work.

1.4 Other deliverables that may be of interest

Deliverable 4.3 is related to other deliverables in the IMPETUS project.

- In WP 1, Deliverable 1.2 lists the requirements for the tool that have informed the development of the UI.
- WP 2 deliverables, D2.1 Platform architecture, requirement specifications and test plan, and D2.3 Platform v2 release + APIs + documentation, set the foundation for the modular structure of the platform and consequently, for the UI, in terms of what information will be presented to the end user (APIs) and the back-end that will power the data feeds.
- D3.4 Tool development final report (description of the tools and their user manuals), and D3.7 IMPETUS toolset (description of the tools' software), determine the status and TRL level of the tools at the end of the project and detail the functionalities that different tools contribute to IMPETUS.
- D4.2 Data analytics and ingestion-time access control final report, since it details the big data "engine" developed and some principles relative to the information provided in order to support interpretation of the alerts generated.
- D7.1 Validation plan and D7.2 Acceptance pilot report, since they provide context for the readers on why it was established that more user personas besides SOC Operators can and should utilize IMPETUS for increased efficiency and matching of their skillset with IMPETUS toolset.

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 IMPETUS end-users

IMPETUS is a platform aimed at providing city authorities with enhanced and improved resources in the shape of state-of-the-art technological solutions, processes, and guidelines to keep smart cities and their citizens safer. However, the range of professionals that share this goal and are responsible for its achievement is wide and heterogeneous. Such heterogeneity mandates the identification of the different key end users of the IMPETUS tool and, more importantly, the specific needs associated with each different user profile. It is also worth mentioning that the analysis of the operational contexts of both partner cities revealed that while they bear substantial similarities, they are not exact replicas; therefore, a certain level of abstraction was applied to define the user profiles. In conclusion, six (6) different user personas have been identified: SOC Operators, SOC Supervisors, IT Specialists, IT Supervisors, Intelligence Planners and Technical Administrators. Figure 1, here below, shows the different hierarchies between them and the most common flows of communication.

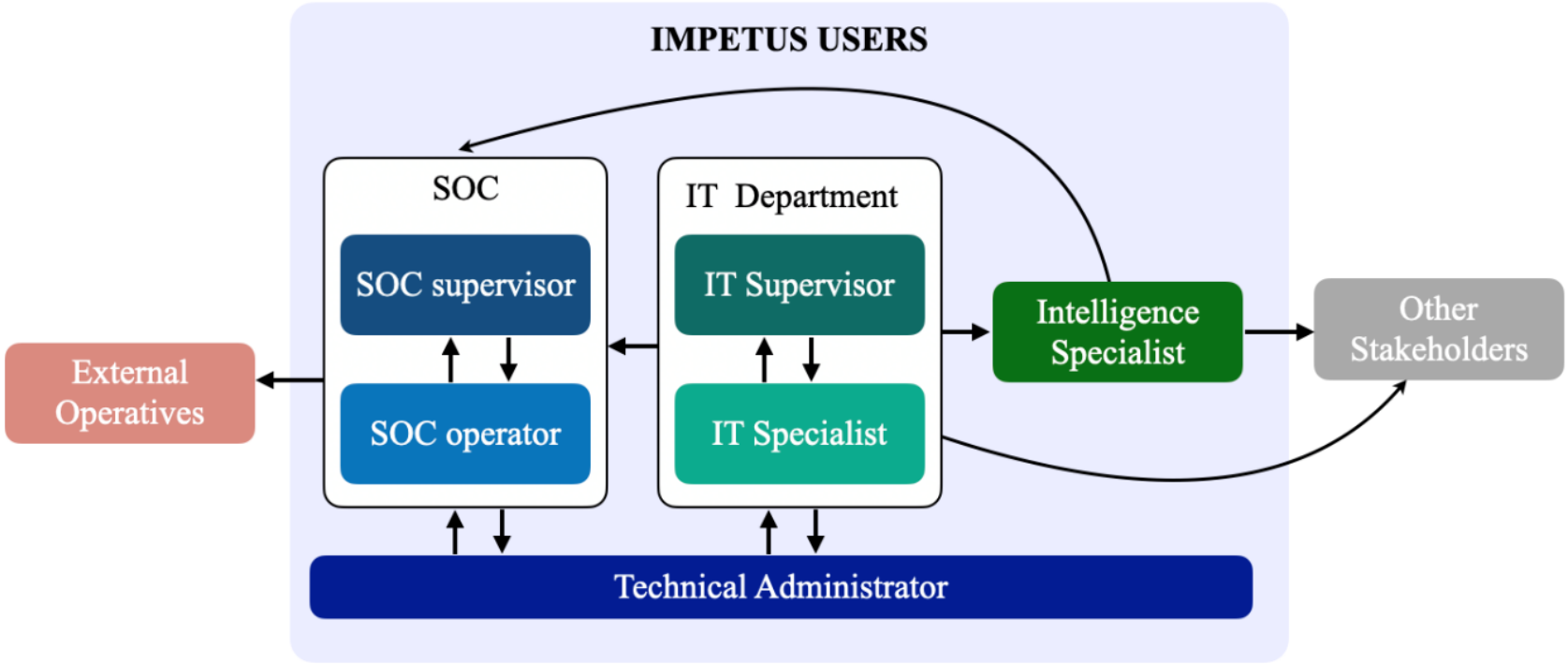

Figure 1. IMPETUS users

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.

The process of identifying the different users and needs was carried out through a number of meetings and questionnaires that the city representatives and end users attended and completed respectively. They were structed around different blocks: core needs, goals and motivations, main tasks and responsibilities, challenges and frustrations, current equipment and tools, work-arounds the issues and frustrations, close collaborators, digital skills, hopes about the future system and fear about the future systems. See Table 3 below as a sample of the template used. The definition of user persons for IT Supervisors and Technical Administrators did not require the same level of detail as the other profiles. Nonetheless, a description of the specifics of their role is included in their individual sections below.

USER PERSONA	
Core needs • •	**Goals and motivation** • •
Main tasks and responsibilities • •	**Challenges and frustrations** • •
Current equipment/tools • •	**Current work-around adopted** • •
Typically collaborates with • •	**Digital skills** • •
Hopes about future system • •	**Fears about future system** • • •

Table 2. User Persona Template

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.

2.1 SOC Operator

Personnel working at the Security Operations Centre (SOC) are responsible for the monitoring of the security of the city and managing and coordinating any incidents or complicated situations that may arise, acting as the command and communications centre amongst several agencies involved and activated as demanded by each varying situation. The number of SOCs and SOC Operators can vary from city to city –they can have one SOC responsible for the whole municipality or, alternatively, multiple ones, each one being only for a specific area and the institutions and infrastructure contained within.

The table below summarizes the aggregated insights gathered from the SOC Operators from both cities.

SOC OPERATOR	
Core needs • Overview of what happens in the city is the most important (situational awareness) • Need to be able to trust the data and information shared • System works correctly (e.g., network connectivity, platforms, telephone, task management systems, radio…) • Clear procedures, checklists, responsive actions • Training/rehearsal • Culture for proper communication • Being a "strong" team player • Being able to build strong relationship with colleagues on the field • Good colleagues. Knowledge, teamwork, work environment • Individually: good headspace. Serenity. No noise (physical or mental)	**Goals and motivation** • Secure buildings, areas, infrastructures in geographical area of responsibility (e.g., City Hall, Harbour…) • Contribute to a safe environment for employees and visitors at official institutions (e.g., City Hall, Harbour…) • Be prepared, respond effectively to unexpected situations • Help colleagues to secure the city • Help other Police forces and emergency players to solve critical situations • Support citizens in "small" issues relate to security and safety • Ensuring public safety • Being relevant in that line of work • Good working environment

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.

SOC OPERATOR	
Main tasks and responsibilities	**Challenges and frustrations**
• Secure buildings, areas, infrastructures in geographical area of responsibility (e.g., City Hall, Harbour…) • Ensure safety for employees and visitors • Contribute to other tasks within the organization • Preparedness and responsiveness • Understand and solve problems related to safety and security coming from citizens and colleagues (mainly via phone call or radio communication) • Coordinate with other agencies • Filter information and forward the important one to the right people (colleagues, supervisors, authorities, citizens, other Police forces, other Emergency actors, etc.) • Provide support to other SOC Operators: everybody is responsible of ALL the issues • "Open" and "close" every intervention in the (log) system • Find out nature of challenge/ task and location • Manage the task (resources, alarms, information in and out) • "Prepare" the intervention: look for complementary information before calling colleagues in action (the higher is the quality of the info shared, the better for the people on the field)	• Noise and interrupting • False alarms • Task saturation – multiple activities/incidents simultaneously • Different screens/tools in the SOC are demanding for new SOC Operators. They get an alarm sound- but do not know which screen the alarm comes from. • For newbies: noise. The expert operators are used to work focusing on the same time both on the issue they are solving and on what the other SOC Operators are doing. For this reason, they all talk loudly. • Obsolete equipment (software, hardware and network connection) • Small location • Sometimes – lack of procedures (or obsolete ones, such as numbers to be called) • The maximum difficulty is to manage a mortal accident • Old and slow system that can be a source of frustration. • Tools malfunctions after office hours when IT personnel is away / free. Not critical, can wait with repairs / restorations.

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.

SOC OPERATOR	
Current equipment/tools • CCTVs • Perimeter control • Fire alarms • Remote access of doors/perimeters • Electronic communication/IT tool for interaction, communication and collaboration with other actors • Journal for reporting • Preparedness plan, check lists and procedures • Several monitors and big screens • Telephone, Smart phone, Satellite phone • Task management software • Map-based traffic management software • Crisis management software. (Alert system) • VHF radio. TETRA radio	**Current work-around adopted** • Prioritizing alarms/incidents by procedures and experience. • Team working • Escalation (in a limited number of cases the supervisors' support is needed) • Alarm • Task initiation • Systems predefined solution proposal. • On-site operative crew sends back information and assessment • Fully continuous working shifts (24/7). • No down time. • 1 operator per shift + 1 supervisor, mainly during office hours
Typically collaborates with • Emergency actors before and during events, and during emergencies. • Other actors within the municipality, both political and administrative. Irregular frequency. • Cooperation with other departments in City Hall at frequent occasions. • Cooperation with other offices of the same organization • Colleagues on the field • Supervisors • Additional agencies and bodies (e.g., Police -including Border Control and Special Forces-, Health Services, Water and Sewerage Agency, Road Traffic Control Centre, Fire & Rescue, Customs, Defence Ministry -mainly regarding exercises-, Norwegian Maritime Authority, Norwegian Coastal Authority…)	**Digital skills** • Average IT skills tested at recruitment • Good knowledge on MS Office • Easy to learn current SOC systems with above mentioned background knowledge. • Trained in specific Traffic management programs

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.

SOC OPERATOR	
Hopes about future system	**Fears about future system**
• A top system that enables increased situational awareness, and prioritizes alarms • An overview map of current status • Higher efficiency • Simpler work processes • A voice-command system (like "Alexa") to open CCTVs, look for a place in the city map, look for a phone number, look for a procedure, etc.) • A broadcast messaging tool • A bidirectional communication tool (in particular to receive images from citizens and colleagues) • City sniffers (gas leakages) • Drone technologies (aerial visual support) • Language translation systems • Location finders	• Increased bureaucracy • Implementing tools not relevant or that demand high workload beyond capacity. • Increased reporting and "paperwork". • Additional responsibilities • A non-user-friendly system, time consuming to be ready to use it • New procedures • Dependency on tools and technologies. • Vulnerability in regard of little humanity in the loop. • Hacking

Table 3. SOC operator insights.

From all the tools the IMPETUS platform aggregates, Weapon Detection (WD), Bacterial Risk Detection (BRD), Physical Threat Intelligence (PTI) and Physical Threat Response Optimization (PTRO) are the best suited for their profile. Communications-wise, they need to be able to transmit efficiently and accurately, amongst other types of information, the details provided by the tool alerts to colleagues in the field or additional relevant stakeholders, either through the IMPETUS chat or through other means of communication (e.g., Telegram, etc.) as established by their protocols and procedures.

2.2 SOC Supervisor

SOC Supervisors are SOC Operators who, after years of experience, have taken on a managerial role that entails overseeing that the SOC works like a well-oiled machine. Their area of responsibility spans from scheduling, shift planning and resource allocation to actively intervening when a situation is escalated to their level or requires all hands-on deck, as well as maintaining an open channel of communication with their counterparts from other agencies and additional stakeholders.

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 detailed summary of their job description is featured in the following table:

SOC SUPERVISOR	
Core needs • Resources • Knowledge and competence. Right use of resources • Being rested and collected • Being his best version • Ensuring that every shift is covered • Ensuring that operators have all they need • Good functioning systems • Good coordination with other agencies and authorities • Leadership skills • Communication skills • Coordination skills • Managerial skills • Security and emergency planning /execution/ evaluation • Systems knowledge (IT, alarm, fire, etc) • Ability to relate to journalists	**Goals and motivation** • Ensure that the team (operators) have the best possible job. Try to bring the best out of them. It affects the results positively. • Good contact with outdoor services. • Lead SOC Operators colleagues and patrols in the field • Ensure public safety and serve the population at large as well as possible • Management and supervision of area of responsibility (e.g., effective harbour management, including considering the amount of traffic -road and vessels-, ensure safe & secure visits to the City Hall -including events-…) • Ensure a proper security culture within security teams (SOC and guards) and the rest of the staff (City Hall staff members), as well as contributing to effective communication & coordination within the institution.

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.

SOC SUPERVISOR	
Main tasks and responsibilities • Personnel responsibilities • Coordinating the SOC team (planning and management work shifts, motivating, solving difficult situation • Security & Safety. • Link with outdoor services • Assessment of staffing needs • Request resources as needed • Make sure the department (operators) is working properly • Contact with other agencies and authorities on management level • Responsible for overseeing operations on the whole • Responsible for coordination between SOC team and security guards • Ensuring compliance to policy, process and procedures • Review and develop processes to strengthen SO framework. • Ensuring coordination with other departments (within City Hall for example) and with emergency agencies through effective communication.	**Challenges and frustrations** • System failure. • Two systems in use where they must log things depending on the nature of the case. • Managing operations without the support of tools because of running updates • The pandemic forced operators to work from home. This wasn't optimal. The operators, in addition to using their PC as they had to download VHF-app (paid service) to be able to communicate with vessels. Nonetheless, they managed to keep the harbour traffic rolling. • Overworked/stressed personnel • Non effective communication among colleagues and/or other staff members • Re-training of SOC Operators • Shortage of trained SOC Operator due to sickness and or vacation

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.

SOC SUPERVISOR	
Current equipment/tools • Telephone • Automatized fire alarm connections • Task management software • Radio • Searches and resource management. • Supervisor own phone (Priority lines) • CCTVs • Perimeter control • Fire alarms • Remote access of doors/perimeters • Electronic communication/IT tool for interaction, communication and collaboration with other actors • Journal for reporting • Preparedness plan, check lists and procedures	**Current work-around adopted** • Dialogue with operators on assessments (scope, conditions, etc.) • Coordination among the operators. follow-up • Prioritizing alarms/incidents by procedures and experience. Ignore less important alarms • Risk of complacency

Typically collaborates with
• Police and Ambulance services at operation manager level. Daily briefings on own intel
• At management level:
  ○ Fire & Rescue
  ○ Police (border control + special force)
  ○ Customs
  ○ Defence ministry (mainly regarding exercises)
  ○ Norwegian maritime authority
  ○ Norwegian coastal authority
• Emergency actors before and during events, and during emergencies.
• Other actors within the municipality, both political and administrative. Irregular frequency.
• Cooperation with other departments in City Hall at frequent occasions.
	Digital skills
	• Same as operator.
	• DSB and the Norwegian fire school recommendation and requirements.
	• Use of own systems. Locus and Vision
	• Searches in Wikipedia, Google and so on
	• Normal digital skills
	• Systems are user-friendly
	• Above average IT skills
	• Good knowledge on MS Office
	• Easy to learn SOC systems with this background knowledge.
	• Should have a more extensive system knowledge- for troubleshooting, increased situational awareness and to command correct responsive action.

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.

SOC SUPERVISOR	
Hopes about future system Use of: • Heat / gas measuring sensors • Seismic sensors • Heightened efficiency. • Better integration with tools at national level. • A top system that enables increased situational awareness, and prioritizes alarms • An overview map of current status	**Fears about future system** • One has to tolerate error messages • Increased bureaucracy • Implementing tools that are not relevant or that demand high workload beyond capacity. • Increased reporting and "paperwork".

Table 4. SOC supervisor job description.

Generally speaking, SOC Supervisors require access to the same tools that SOC Operators do, plus the addition of the Human Computer Interaction (HCI) tool that will provide them with a more accurate picture of the mental, physical and emotional state of their teams while on shift.

2.3 IT Specialist

IT Specialists are responsible for attending the IT requests of the staff in their institution/agency, but also and more importantly, are tasked with safeguarding the safety and robustness of the networks, connections, and systems in the municipality. In this endeavour, they can greatly benefit from leveraging tools that aide them and expedite the process of keeping up to date with the new and everchanging threats often brewing in the dark web, identifying if their systems have potential exploitable vulnerabilities and patching them ideally pre-emptively or as fast as possible in case of a potential cyber-attack.

The table below goes into further details and elaborates on the particulars of the IT Specialist job.

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.

IT SPECIALIST	
Core needs • Understand the threat level on the city assets • Identify trends in cyber threats • Detect nefarious activity • Find -quicky- a countermeasure when a weakness or vulnerability has been detected	**Goals and motivation** • Passion for IT • Sense of responsibility
Main tasks and responsibilities • Daily monitoring of web sources for learning about threats • Conduct regular vulnerability analyses • Improve network configuration to increase security • Keep good knowledge of the city network and assets • Manage Network Detection Tools	**Challenges and frustrations** • The network changes all the time • The city is deploying smart services with too little focus on cyber security • Network detection tools raise too many false alarms • Old software equipment to be kept "alive" because of lack of innovation and limited IT skills of the end users (e.g., politicians and authorities) • Limited budget • Bureaucracy • Difficulties to relate with end users because of the different background
Current equipment/tools Non-disclosable	**Current work-around adopted** • Use personal time and computer to access online resources blocked in the SOC
Typically collaborates with • System administrator • Other departments • End users	**Digital skills** • Expert • Learns new skills easily
Hopes about future system • More efficient vulnerability analysis process	**Fears about future system** • IoT everywhere makes the network impossible to monitor • Implementation issues • Feasibility

Table 5. IT Specialist job

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 2 tools that are more directly related to their tasks and responsibilities are the dark web detection tool, namely Cyber Threats Intelligence (CTI), and the tool that scans for vulnerabilities in the system, detects them and proposes countermeasures to fix them: Cyber Threats Mapping (CTM). Communication with other stakeholders and profiles is used on a need-to-know basis, namely when they need to be warned about potential or real problems or some action is required from their side to ensure safety (password changes, installation of new features, protocol updates…).

2.4 IT Supervisor

The IT Supervisor manages and supervises the teams of IT Specialists, recruit new staff and provide training whenever required. It is also in their purview to perform operational assessments and provide support to the IT Specialists. As administrators, the ultimate responsibility of assuring the cyber security of the systems lies with them, therefore, regardless of whether the IT Specialists can assign to themselves specific computer security - tasks or it is the supervisor who distributes them, they need to have a complete vision of everything that their department is working on, assess the task log and ensure its correct prioritization.

IT Supervisors are also in charge of budgeting and need to foster a collaborative environment with their personal to find innovative solutions for all IT issues, maintain logs and keep all hardware and software processes according to security requirements.

In terms of their level of interaction with IMPETUS, IT Supervisors need access to the same tools as IT Specialists (CTM, CTI), and to the communication channels relevant for their job (chat or email in case they need to convey information to other stakeholders). It is also at the IT Supervisor discretion if they would like their teams to utilize the HCI to be able to empirically assess how their workload affects them at different points in time.

2.5 Intelligence Analyst

The role of Intelligence Analyst can be carried out by different profiles in different organizations –it can be a hat that some SOC Supervisors also wear or be a completely independent person in a different department of the municipality structure. What does not change, however, is their list of responsibilities and purview: Intelligence Analysts are tasked with scouring the open web in search of discreet signals that can provide them insights into an array of relevant areas. These insights can be pre-emptive in nature, such as the early identification of potential threats to institutions, infrastructures or people, tracking public sentiment about specific topics, detecting chatter related to the organization of public demonstrations or sizeable gatherings or identifying hate speech about vulnerable groups; or reactive, such as assessing the public reaction or fallout after specific events, or monitoring how a situation evolves.

Once relevant insights are detected and assessed, the Intelligence Planner shares them with the SOC to give them advance notice of any intelligence that can translate and evolve into a situation that is likely to have offline repercussions or cause disruptions that they will have to manage. The intelligence gathered can also be shared with additional stakeholders (politicians, other emergency services and authorities…) that can benefit from receiving that knowledge. See the table below for further details on the Intelligence Analyst role.

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.

INTELLIGENCE ANALYST	
Core needs • To find relevant data and specific information about the object of the investigation (a person, a group of people, “drug-dealing" activities, thefts, non-authorised cars/motorbikes races, non-authorised gatherings and demonstrations, etc.) • To find relevant data among all the noise generated in social media. • To understand the general feeling and considerations of the population around certain topics. • To share –quickly- relevant info to colleagues, supervisors, authorities	**Goals and motivation** • To understand the general mood of the population against specific situations around certain topics or keywords • To identify possible threats, hate speech and negative sentiment in social media and the Internet in general • To identify criticism to public figures (such as the mayor), political parties or institutions • To identify relevant messages in very popular topics (filtering) • To identify relevant messages in non-popular topics (locating) • To detect relevant info and evidence of criminal activities
Main tasks and responsibilities • To identify possible threats to the city and its citizens • Guarantee and support the correct planification of the security of public figures and institutions • To draft reports of illegal activities • To monitor risky areas • To Investigate about “suspicious” people • To plan, coordinate and manage intervention on the field	**Challenges and frustrations** • Manual tasks that are very time consuming • Diverse data sources, many messages per data source • Multiple languages, some of them not very familiar to them • Obsolete technology • Too restrictive privacy policy / law on searching for suspicious persons • Internal restrictions on the navigation of sites and databases useful for carrying out investigations that are too severe • Sometimes lack of procedures and protocols
Current equipment/tools • PC • Social media accounts • Lack of any tools to monitor and analyse social media • Defined operations and procedures (currently only guidelines are available)	**Current work-around adopted** • Manual websites and social media browsing • Read and interpret all the messages they consider relevant
Typically collaborates with • SOC Supervisor ○ Send a -brief- report related to the findings of their investigation • SOC Operators • Police	**Digital skills** • Proficient in Internet browsing • Social Media experts

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.

INTELLIGENCE ANALYST	
Hopes about future system	**Fears about future system**
• To have a tool that automatically assists them in finding relevant information (and more especially negative messages) • To have a unique instant messaging tool • To have procedures and protocols • To have CCTVs with AI or something like face-recognition • To have CCTVs able to detect anomalies	• Lack of relevant data sources • UI may be too complicated for some people ○ Training needed • False positives • No technological innovation in the equipment

Table 6. Intelligence Analyst role

The SMD tool is the clear match for the Intelligence Analyst, and the IMPETUS chat the fastest way to communicate relevant insights to the SOC. Other means of communication, like email, would be the most adequate to share the information with additional stakeholders.

2.6 Technical Administrator

As far as IMPETUS is concerned, the role of the Technical Administrator is understood as the professional within the IT department who, after receiving proper training, becomes the IMPETUS expert and is the main go to person for the configuration and tailoring of the IMPETUS platform for the end users. The Technical Administrator oversees the creation/activation of user IDs for IMPETUS, ensuring the tool works seamlessly with existing systems once deployed and configuring that each end users has access to the tools they require or want. Generally speaking, the most natural fit between each of the different profiles and the tools is the one represented in Figure 2 below. This can be understood as the “default” distribution of IMPETUS tools amongst 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.

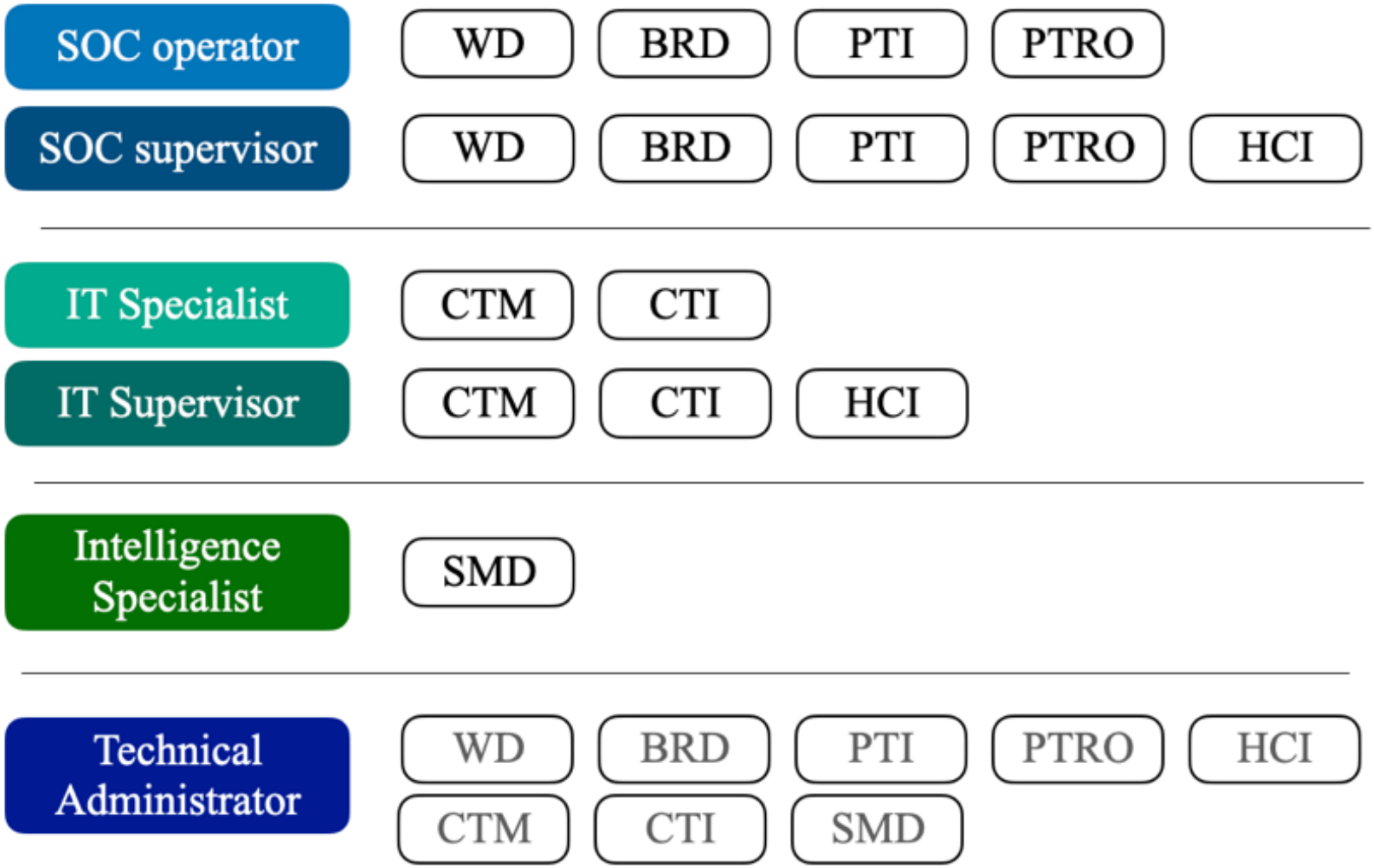

Figure 2. Matching of profiles and tools

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.

Nonetheless, this distribution is by no means static and it can be freely adapted, with the assistance of the Technical Administrator, to reflect virtually any other combination of tools per user. Configuration-wise, IMPETUS can be understood as a fully-configurable architecture, where each end-user chooses the tools that are more relevant for them.

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 IMPETUS Interface

3.1 Introduction

User interfaces are a static representation, a design exercise used to map out and visualize in which way information will be displayed in front of the users. Coming up with a comprehensive and user-friendly interface is a complex process due to the fact that all different pieces must fit together structurally and visually, with the addition of having to provide easy and intuitive pathways to move from one piece to the other.

The IMPETUS UI, along with the underlying system architecture, have been developed from a series of meetings with CPAD and OSL to get their initial thoughts on what the system could look like and a series of dedicated meetings with tool providers. Tool providers offered their input as to what information they would be sharing with the IMPETUS platform and made suggestions on the best way it could be displayed. Different versions were proposed and after each iteration, adjustments were made to better match user needs.

3.2 Evolution

The first version of the IMPETUS UI took as a starting point the templates provided by the supporting platform, Snap4city. As it can be seen in Figure 3, it consisted of a number of tiles in a dashboard that would lead to each specific tool's section within the IMPETUS UI, as can be seen as a sample in Figure 4.

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.

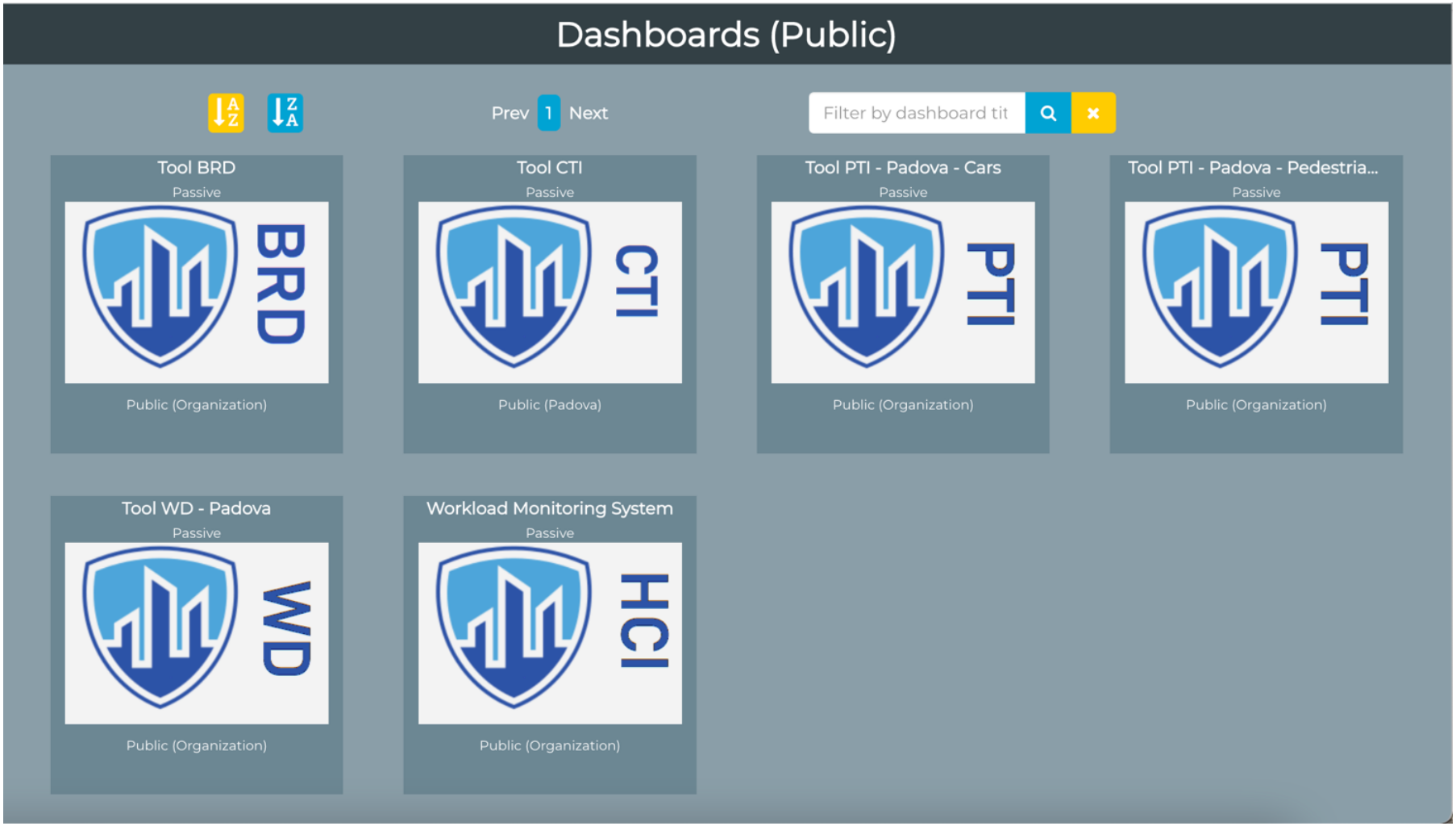

Figure 3. Look and feel of first dashboard

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.

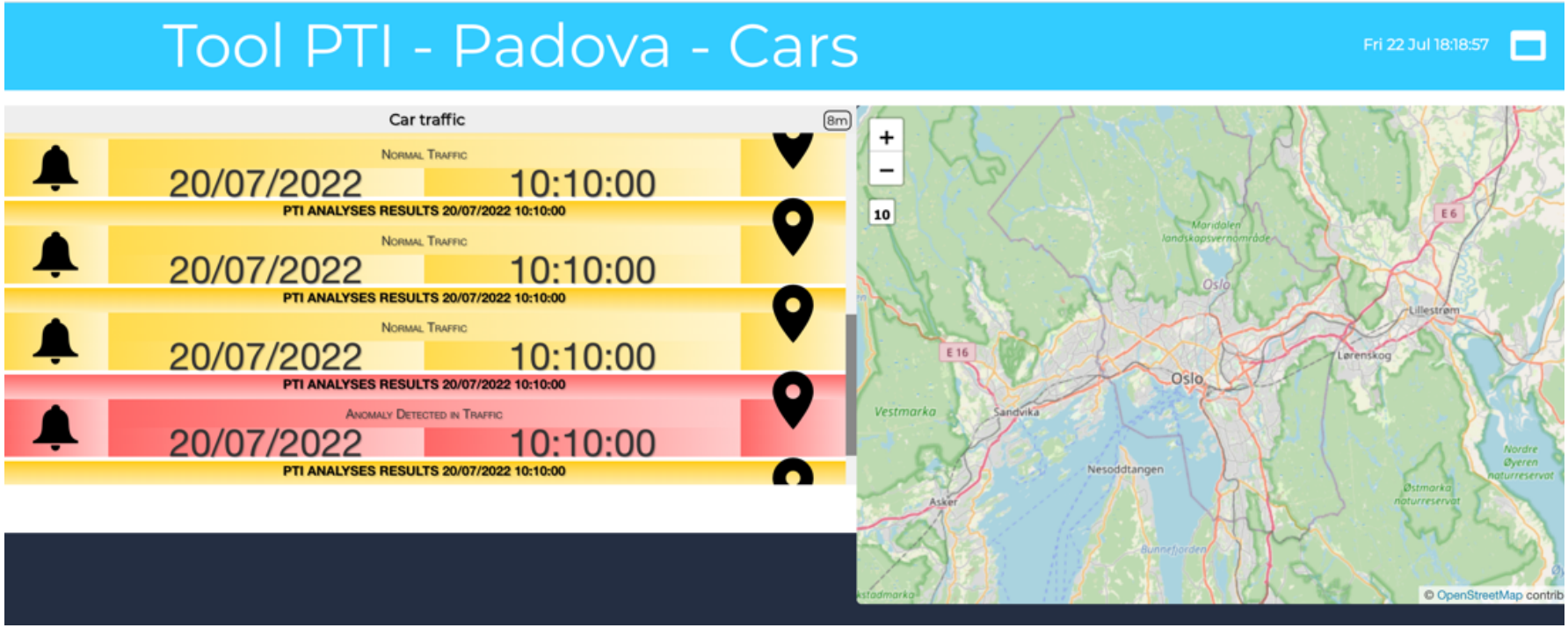

Figure 4. Initial PTI interface

Even though these interfaces were fairly basic, they were intended to provide a preliminary yet tangible starting point to kick-start the UI design process. They were useful in so far as they allowed the consortium to make the following determinations:

- For SOC users, it is not feasible nor advisable to have their whole screen occupied by IMPETUS when they are not actively engaging with it (i.e., right after they have received an alarm notification). They need, however, to still be able to receive alerts efficiently.

- Information needs to be displayed in a clearer, simpler way, with a style that is less cramped and allows for breathing room on the screen.

- The dark mode is more suitable to the environment of a SOC.

From this point, a second iteration of the UI was developed, as can be seen in Figures 5 and 6. The main addition was a side bar, which is to be visible at all times and that will act like the alert centre. Whereas the whole IMPETUS platform will be deployed as a web application accessible through any browser, the side bar requires installation on the end user computer.

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.

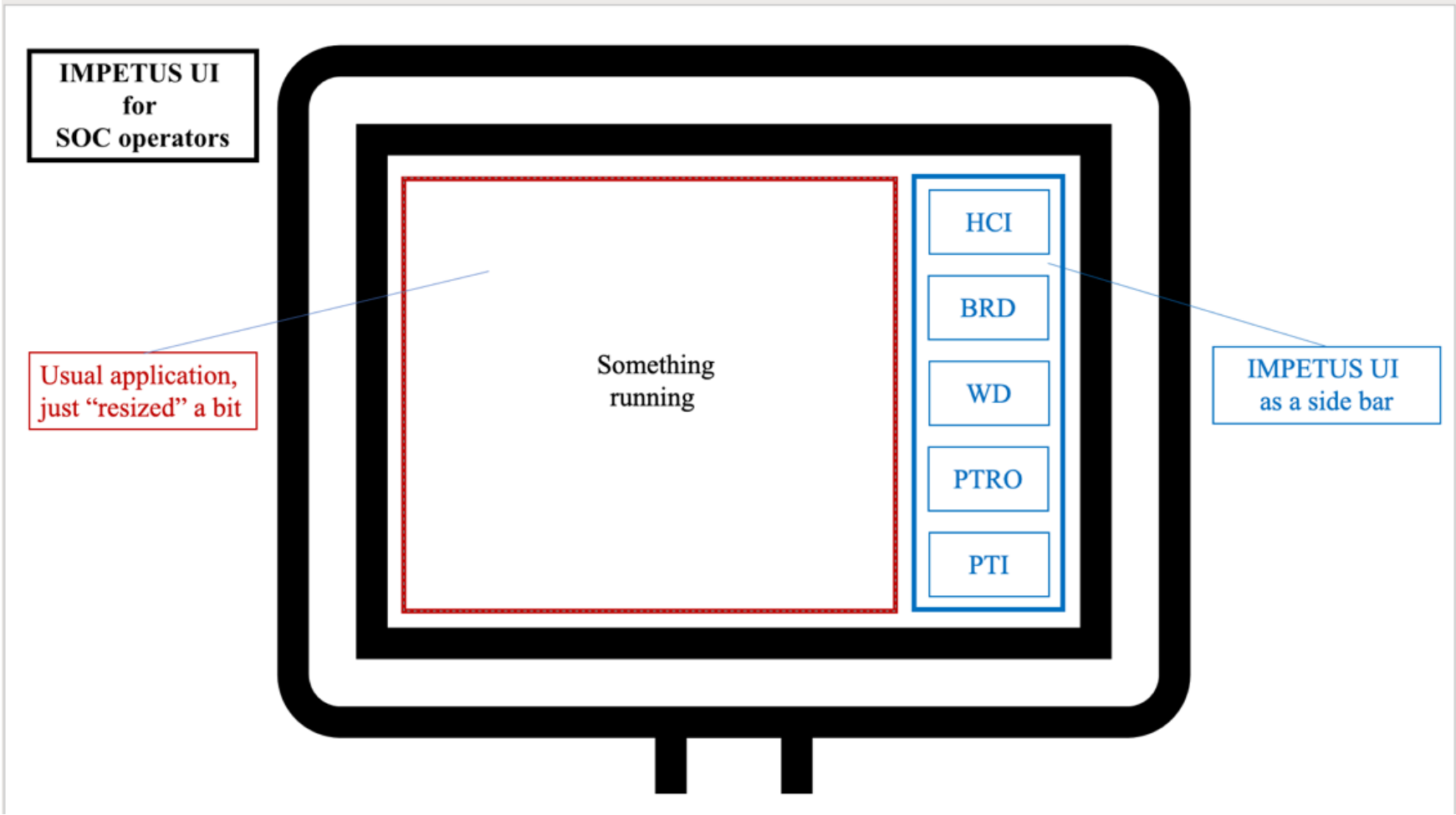

Figure 5. Original Side bar screenshot

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.

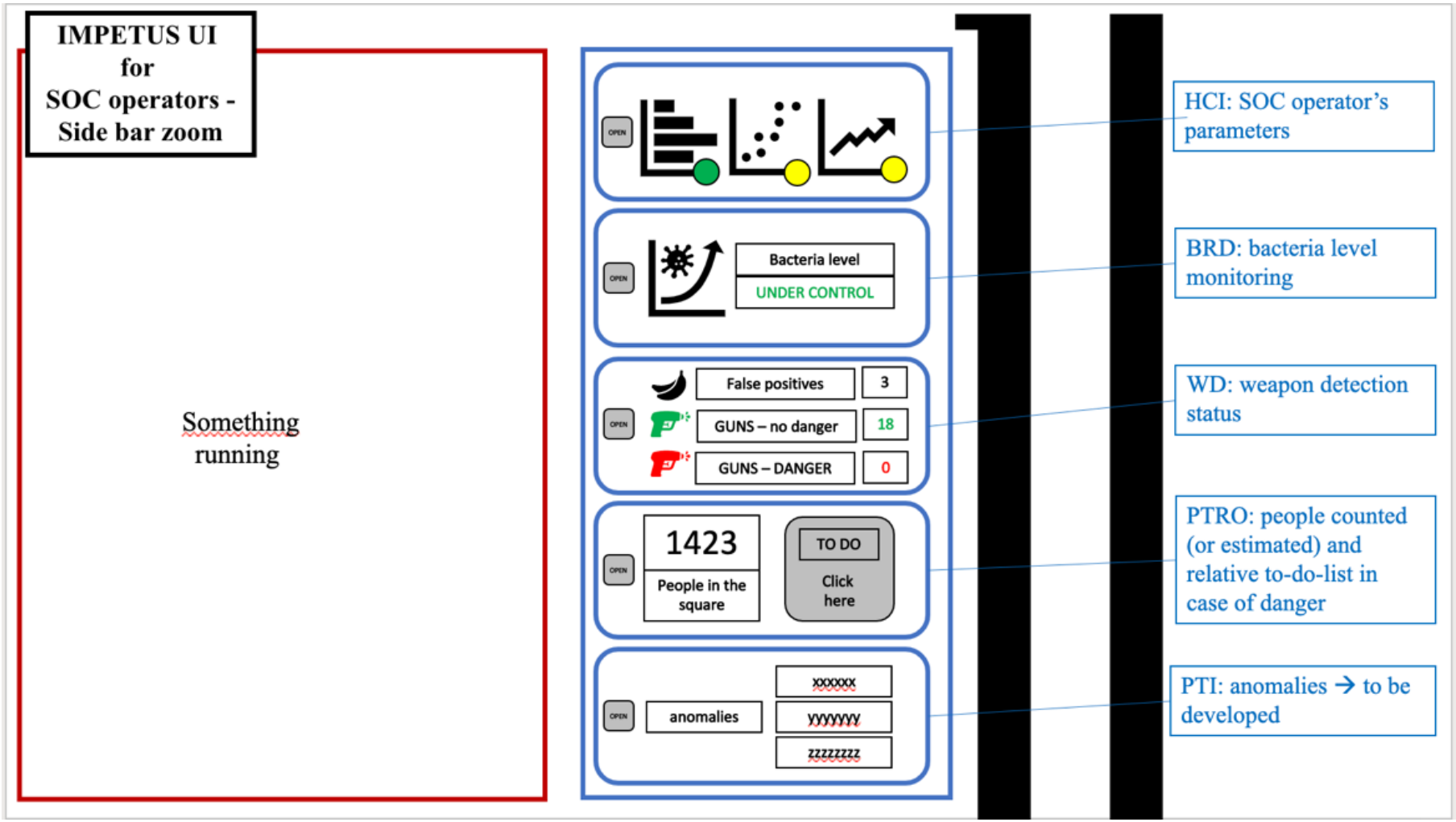

Figure 6. Original side bar details

The option was considered to have a "preview "of the key alert details displayed on the side bar when clicking on the alert notification. This would be presented as a popup as shown in Figure 7.

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.

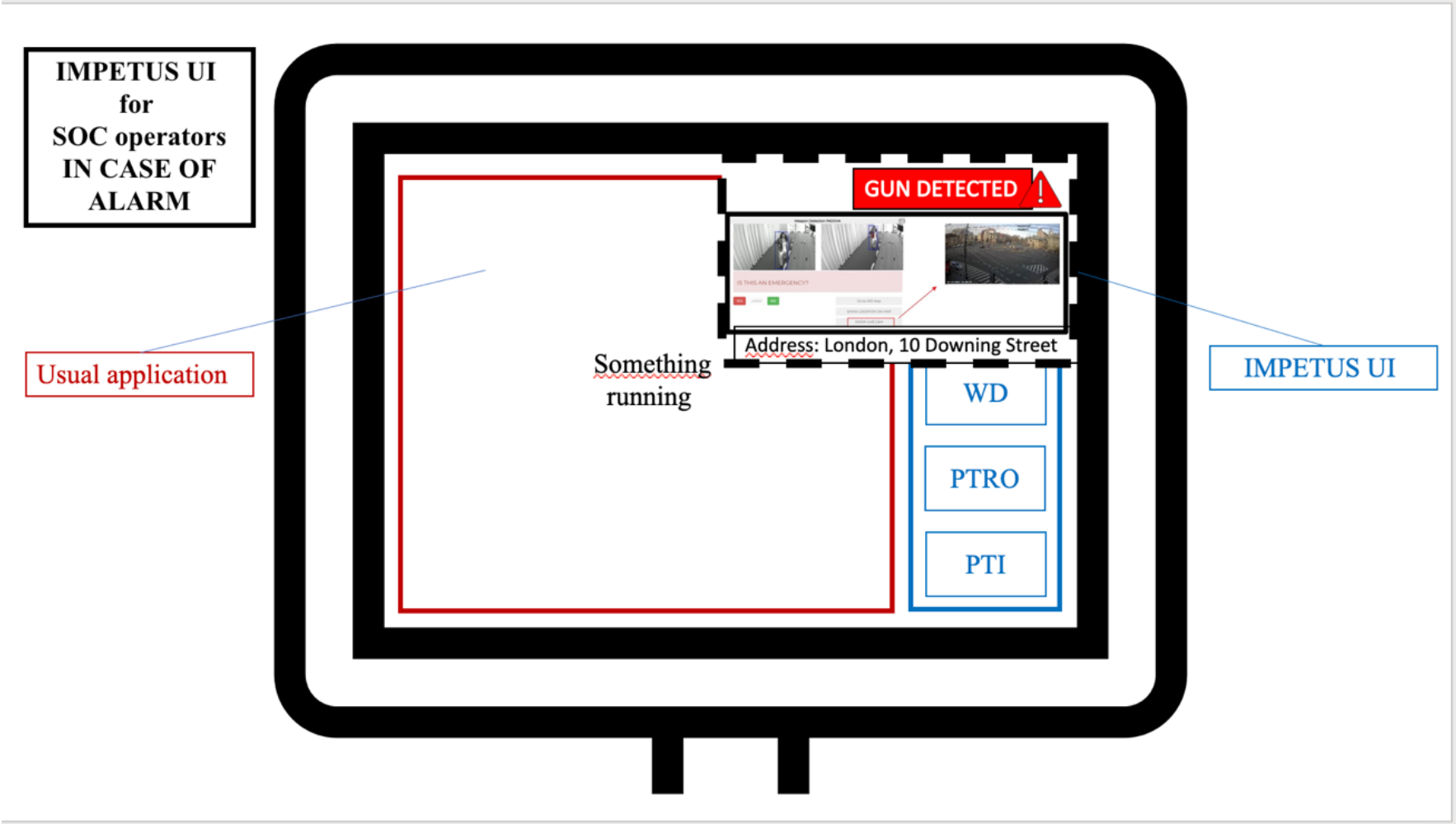

Figure 7. Original alert preview

If was finally assessed that SOC Operators would in all likelihood still go to into the IMPETUS dashboard to gather all the details about the alert before making a determination on how to use handle it, therefore making the previsualization potentially a redundant step.

A final decision was made to show in the side bar an icon representing each tool that will display when there is an alarm, and an automatically updating list of the alerts, text only, providing basic details on each one (tool, title, timestamp) for situational awareness (screenshots can be found in Section 5.3.1).

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.

3.3 Integration Levels

The aim for the development of the UI has always been to find the simplest and the most effective way for end-users to interact with the tools, namely that they will be able to get all the information needed, react quickly and share info with other stakeholders. It is important for IMPETUS to display exactly what is needed, nothing less and nothing more, particularly to avoid noise in the interface or to present redundant information that can be accessed in a clearer and more comprehensive manner within the proprietary portals of the tool providers if needed. To facilitate access, tool providers have created the adequate IMPETUS section/user profile within their own platforms according to the privacy and user policies previously determined.

This principle explains the varying levels of integration of the tools with IMPETUS. Two major groups can be identified: full integration with IMPETUS (dashboard + alerts) and partial integration (alerts).

- **Full integration with IMPETUS UI** (tools without pre-existing proprietary UIs or tools with pre-existing proprietary UI that requires deeper integration with IMPETUS for maximum efficiency).

    - *WD tool:* the AI in the WD tool scans the footage provided by cameras to detect the presence of weapons in the video images. To protect privacy, the AI systematically anonymizes people's faces, blacking them out. The face of a person only becomes visible when they are brandishing or carrying a weapon. In that case, the SOC Operator is sent an alert with the problematic images and their geolocation, and is given the option to confirm whether the person carrying the weapon effectively constitutes a threat (an armed police officer would not qualify as such, for instance). If an emergency is declared, the alert is shared automatically through Telegram with officers in the field.

    - *PTI tool*: the IMPETUS UI visualizes the results yielded by the Big Data Analytics algorithms for anomaly detection of the data provided by the sensors in both cities. The UI shows geographic position of the sensors and the time-dependent values observed. When no anomaly has been detected, the platform shows graphs of the continuous evolution of the data and a display of the location of all the sensors/geographical areas. When an alert is triggered, the platform zooms in on the area of concern, all the graphs are updated to show the relevant data associated to the alert and displays which of the different variables carry the most weight in the anomaly detected.

    - *BRD tool*: IMPETUS will show the continuous results of the data gathered from the sensor and send an alert when the concentration levels surpass the acceptable threshold and suggest a list of immediate actions to be carried out while awaiting the intervention of the specialists.

    - *PTRO tool*: the PTRO acts as a repository of simulations for the evacuation of public areas of specific interest for the cities. Aimed at SOC Operators, in case of an emergency (maximum capacity of a square exceeded, need to evacuate due to a fire hazard or accident…), the PTRO provides egression routes and strategies to assist in the management of 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.

Figure 8 below represents the user journey (understood as the steps a user may take to reach their goal when using a particular website) within the IMPETUS platform for fully integrated tools.

Figure 8. User journey for fully integrated 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.

- **Partial integration with IMPETUS UI** (tools with a previous fully developed proprietary UI)

    - *HCI tool*: IMPETUS receives an alert when the end users wearing the sensors display sings of emotional, physical, or mental overload. To view the details, the user is redirected to the HCI proprietary UI.

    - *SMD tool:* the user creates a project within the SMD tool proprietary platform and receives an alert through the IMPETUS UI once the analysis of the project has been completed or if there has been any kind of error that has prevented the completion of the project. The user goes back to the SMD tool platform to visualize the completed analysis and insights extracted.

    - *CTM tool*: the user receives an alert through IMPETUS once a vulnerability has been detected. The key identifier details are featured in the alert, and the user can access the CTM UI to find additional details and remedial measures.

    - *CTI tool*: the CTI platform has the infrastructure to list threats, categorize them, provide all the necessary details, assign them to different users and track if they are untreated, in treatment or resolved. The integration with IMPETUS displays an alert for new untreated threats so the *user knows when to pivot to the tool's own exteernal UI to analyse them.*

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 9 below illustrates the user journey for IMPETUS users when interacting with partially integrated tools.

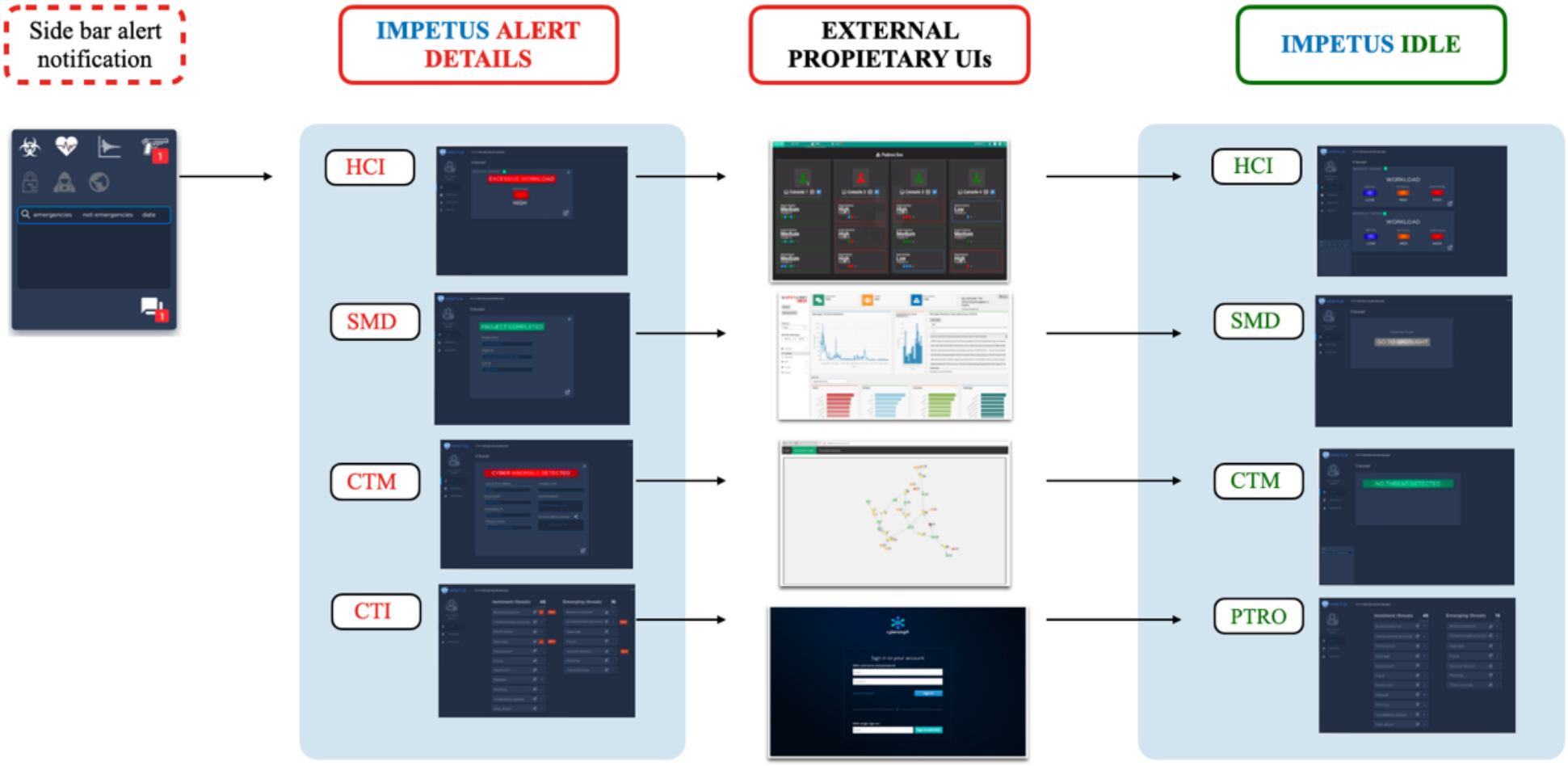

Figure 9. User journey for tools with proprietary UI

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.

3.4 UI guidelines

Even though the levels of integrations with IMPETUS vary as described in the previous section, the UI design followed as a whole a number of straightforward and widespread design principles such as:

- Dark mode to suit the illumination working conditions of SOC Operators
- Minimalism to increase clarity and simplicity
- Easy navigation
- User-experience placed at the forefront of the process

However, the following 2 guidelines have been taken into particular consideration when designing the UI:

- Consistency: to facilitate user experience, the UI has been designed trying to maintain and repeat the same structure in as many of the tools' dashboards as possible within the possibilities determined by the components and behaviours of the tools. This principle mainly applies to the distribution of different components of the alerts in the screen (title of the alert, date and time stamps, geolocation, lists of alerts icons, resolve button…).

- Modularity and personalization: it is a central requirement that the UI allows for customization and variations so each user profile can tailor it to their needs. With the assistance of system administrators, tool tiles can be added or removed as required from the home page, and colour coded according to their relevance to each user.

3.5 Description of the main elements of UI

Besides the login interface, four main areas can be identified in the Impetus UI: the side bar, the home page, the chat, and the tool alerts/dashboards.

3.5.1 Side bar

The side bar is designed mainly with SOC Operators and Supervisors in mind, to solve the "screen real state" problem. SOC Operators need to be able to decide what they need to see on the main area of their screens, while at the same time they need to be able to see when an alert comes in. The side bar is optional for the other profiles.

The side bar contains:

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.

- *Icons for each of the tools (Figure 10)*. The alerts are first displayed by having the icon pulsate in red to capture their attention since the human eye is prone to detecting movement over static objects. Once the user clicks on the alert to see the details, the pulse stops.

Figure 10. Tools icons

- *Log of the alerts*: ongoing and solved, displayed according to the following structure: “Tool – date and timestamp – alert details". The goal is to be able to identify in one place with one glimpse what is happening in real time. As it can be seen in the following sections, tools' alerts feature a “RESOLVE” button, which will translate in as that specific alert showing as “resolved” in the alerts log as Figure 11 shows.

- *Chat icon*: it displays if the user has new messages and by clicking on it, the user is directly brought to the chat 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.

Figure 11. Side bar screenshots.

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.

3.5.2 Home page

The home page is the welcome page, the first thing the user sees once he has logged into IMPETUS. It provides a summary of all the tools the specific user will have access to or use. This page is 100% modular and can be configured to meet the working needs of any number of user profiles, and even allows for the incorporation of additional tools in the future if so needed.

The vertical list of icons on the right side is a constant throughout the whole IMPETUS platform to allow for seamless navigation between the tools within the UI. As it can be seen in Figure 12, the icons on the right will change to blue. The tiles in the middle part "introduce" the tools to the user and provide a short description of their individual purposes and also take the user to the tools IMPETUS dashboard. The tool providers' external proprietary UI can also be accessed directly from the IMPETUS home page through the external link icon at the bottom right of each tile ( ). With user ID integration, IMPETUS constitutes a single point of entry for the external UIs as well.

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.

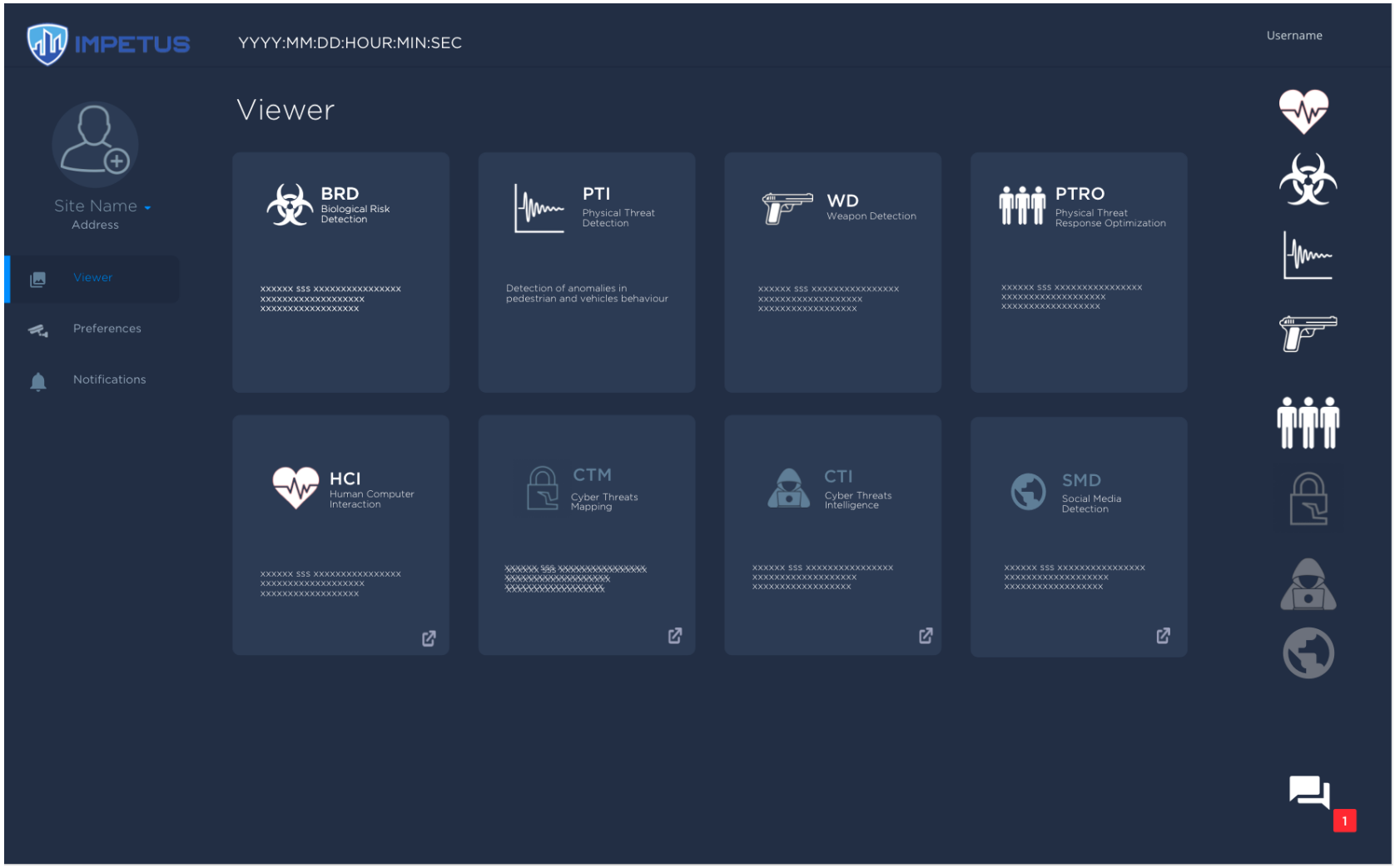

Figure 12. Home page screenshot full access

The colour scheme is based on the prioritization of interactions between users and tools: all the tools a specific user will be primarily responsible for are shown in white, while the ones in darker grey are for consultation purposes. Once again, these settings are 100% customizable.

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.

3.5.3 Chat

The chat is one of IMPETUS's key functionalities. It allows all the users that are connected to IMPETUS to communicate instantly with one another. Shortcuts to the chat can be found in the side bar, in the home page and in each of the tools' dashboards. There is a general channel combined with chats dedicated to each specific tool.

Besides free text, it also allows for the details of each alert to be shared automatically when clicking on the share icon , along with a comment from the user sharing the alert. It also supports sharing rich formats like images or documents. Figure 13 shows a screenshots of the chat look and feel.

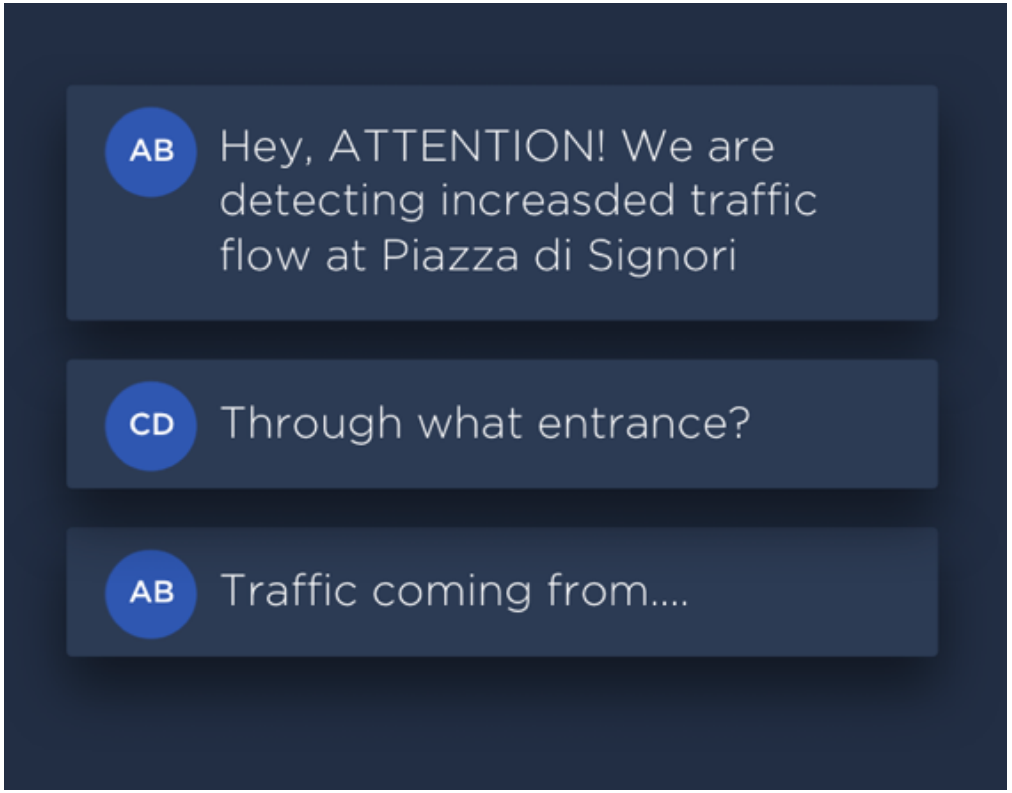

Figure 13. Chat screenshot

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.

3.6 Tools screenshots

The following section provides screenshots of the dashboards of the tools and the alerts. The tools are grouped according to the main profile that will be using them: SOC Operators, IT Specialists, Intelligence Analyst and Supervisors (SOC and IT).

3.6.1 Primary profile: SOC Operators

Tools related to live events requiring immediate attention and action:

3.6.1.1 Weapon Detection (WD) Tool

When the AI of the WD tool identifies a weapon in the CCTV feed, an alert is sent to the SOC Operator with all the information required for the end-user to assess the situation quickly and be able to determine if an emergency needs to be declared. As Figure 14 shows, the SOC Operator receives the GPS location of where the weapon has been detected, a still image of the weapon, a video of the footage and how many minutes and seconds have passed since the weapon has been detected.

Figure 14 also shows how they can click on the “YES” button, automatically sending all the details of the alert to the patrols on the field through telegram. They can also mark the alert as not an alarm and change their decision one way or another with the “UNDO” button (Figure 15). If a declared emergency gets cancelled, patrols on the field also receive the corresponding message. An example of the Telegram chain of messages is presented in Figure 17.

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.

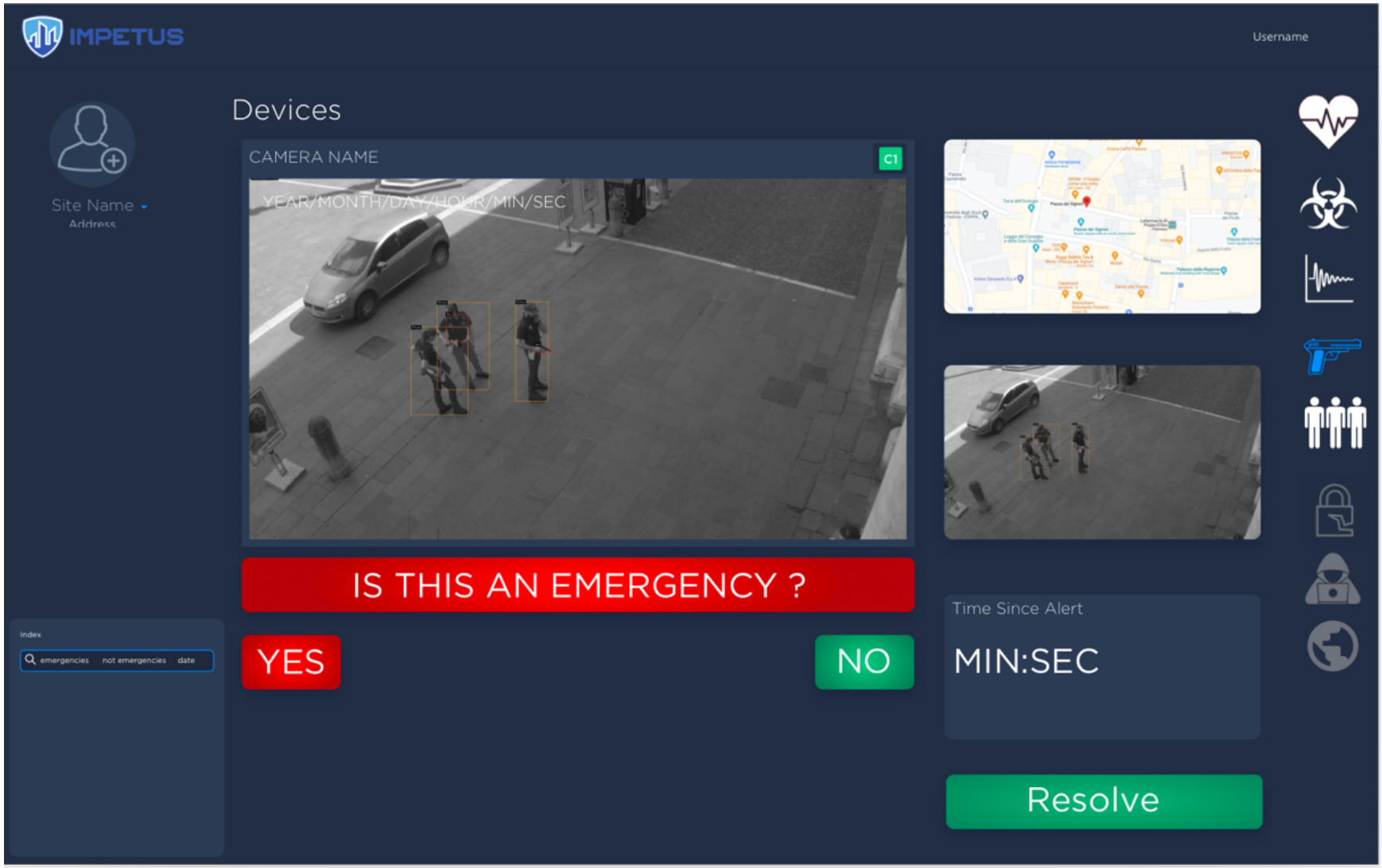

Figure 14. WD Emergency determination

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.

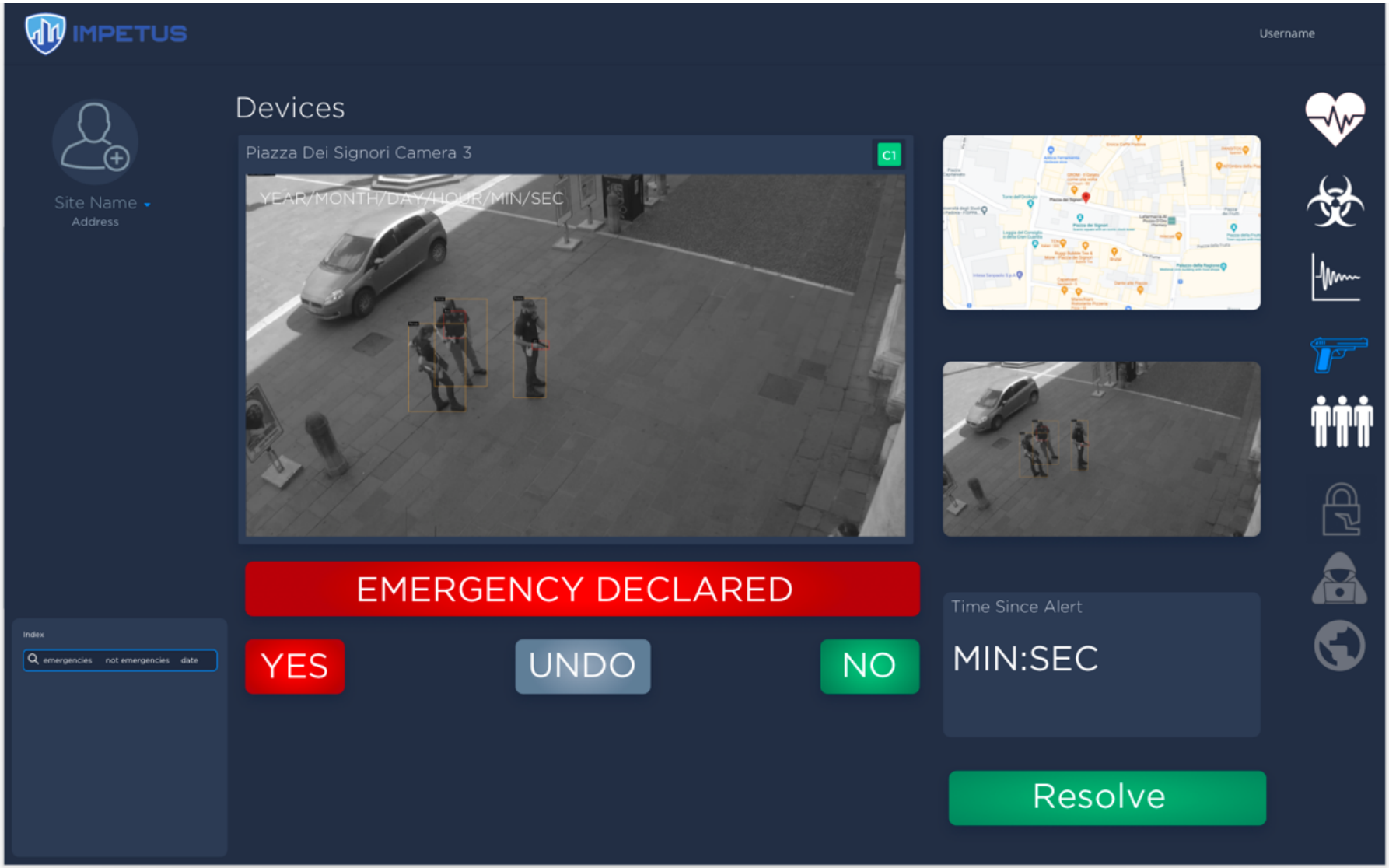

Figure 15. WD emergency declared

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.

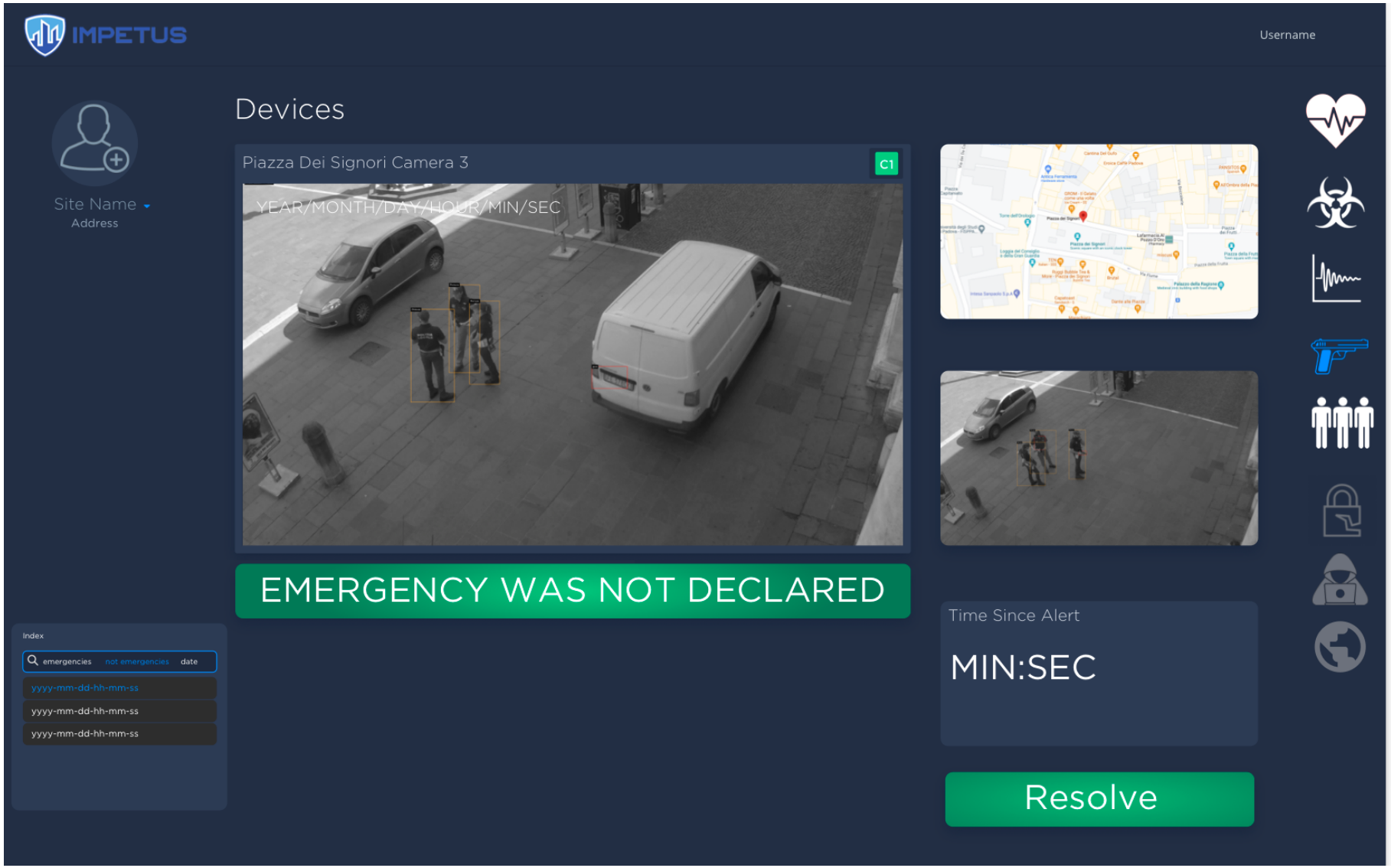

Figure 16. WD Emergency not declared

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.

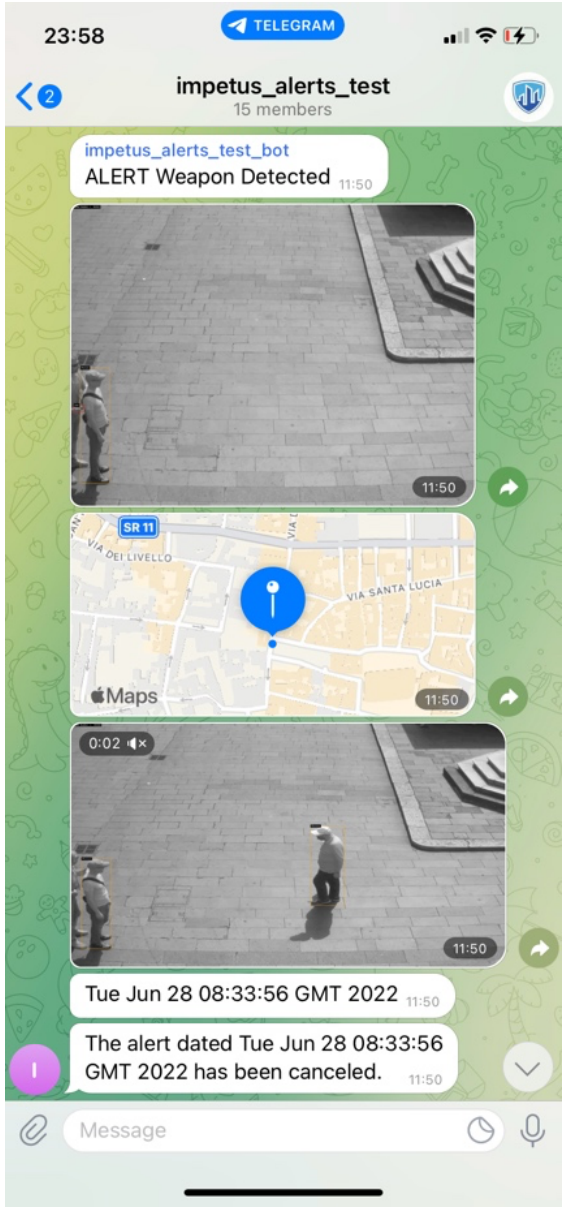

Figure 17. WD Telegram alert chain

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.

3.6.1.2 Physical Threat Intelligence (PTI) Tool

The PTI UI is tailored to each city to display the variables that are relevant in each municipality, as well as the corresponding maps, naturally.

For Oslo, the city is divided into geographical areas and for each area the variables monitored are the following:

- average delay of buses (in minutes),
- concentration of buses in the area (absolute number),
- percentage of buses out of order and
- percentage of buses blocked due to traffic jams.

The map on the top right shows through colour coding of pins in what area the alert is situated; the graphs below display the evolution of each variable over time up until the moment when the alert is triggered and the section in the middle zooms in onto the affected area and shows the causes for the alert in a pie chart for easier visualization and comprehension (Figure 18).

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.

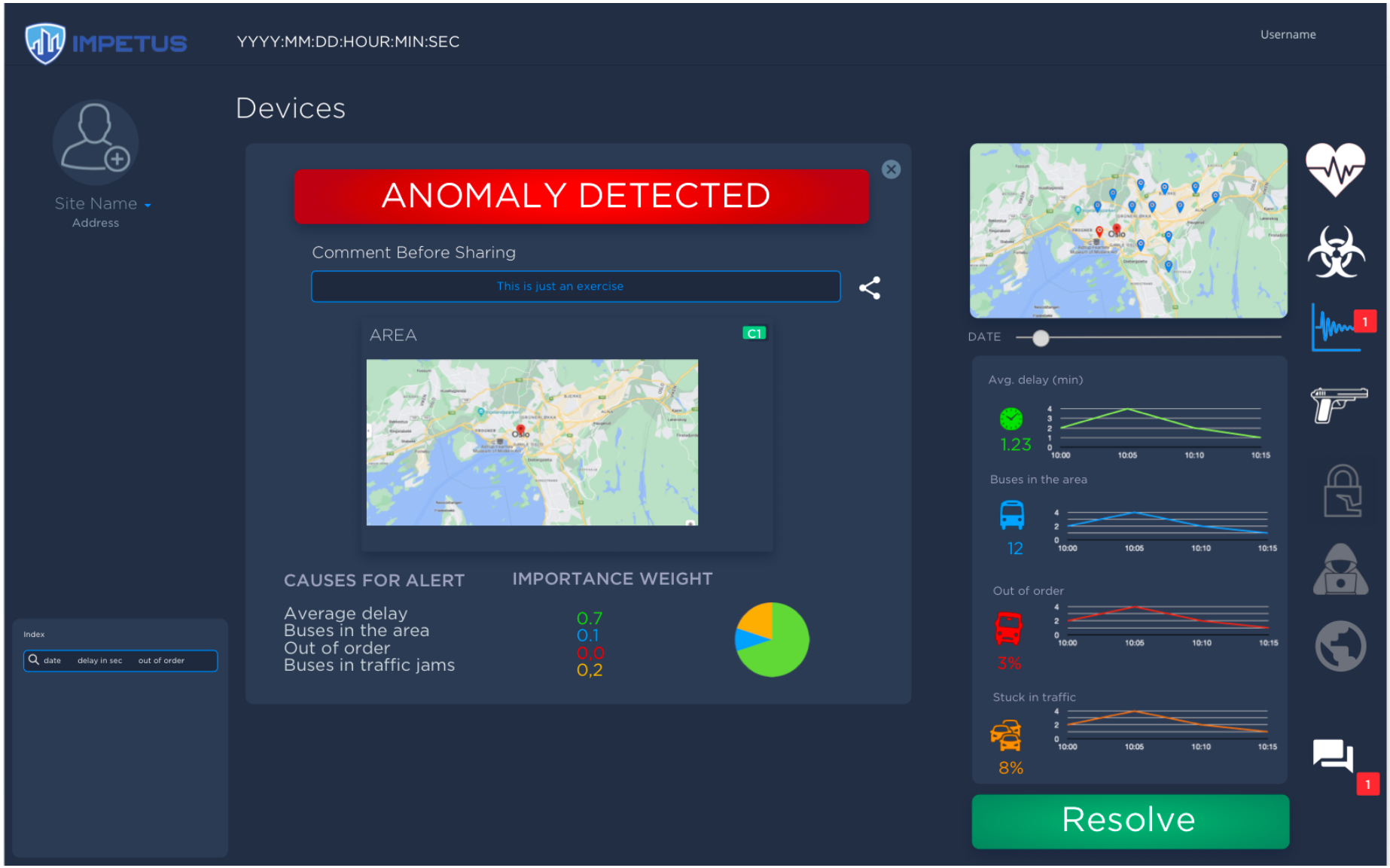

Figure 18. PTI alert in Oslo

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.

For Padova, the geographical areas are determined by the sensors placed around the city, which provide information about:

- Pedestrian flow (in Piazza dei Signori)
  - incoming pedestrians
  - outgoing pedestrians

- Vehicles in circulation (Piazza dei Signori and other points of interest).
  - incoming vehicles
  - outgoing vehicles
  - unknown vehicles.

The elements are distributed in the screen (as seen in Figures 19 and 20) replicating the same pattern as show in Figure 18 for 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.

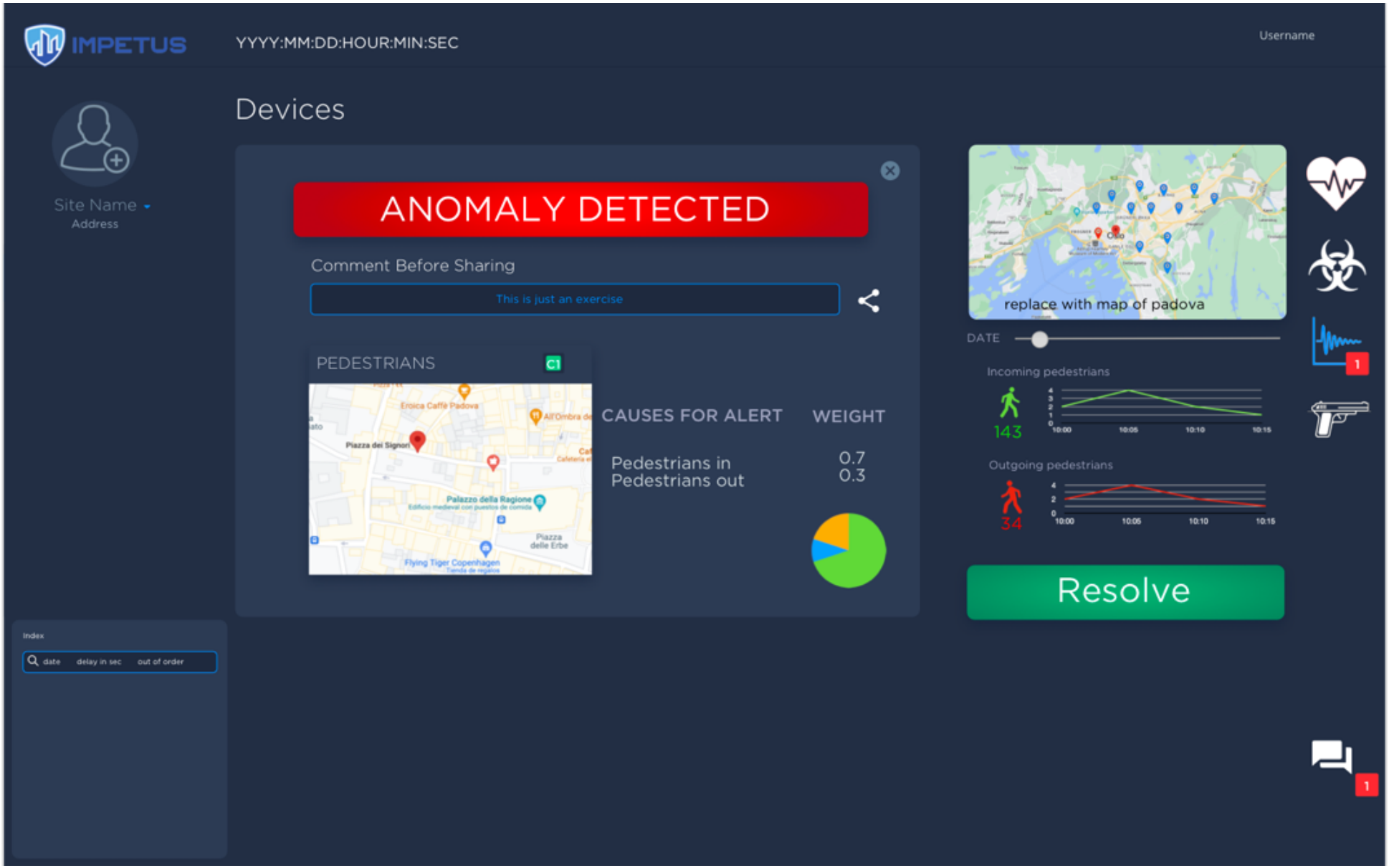

Figure 19. PTI Padova for pedestrians

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.

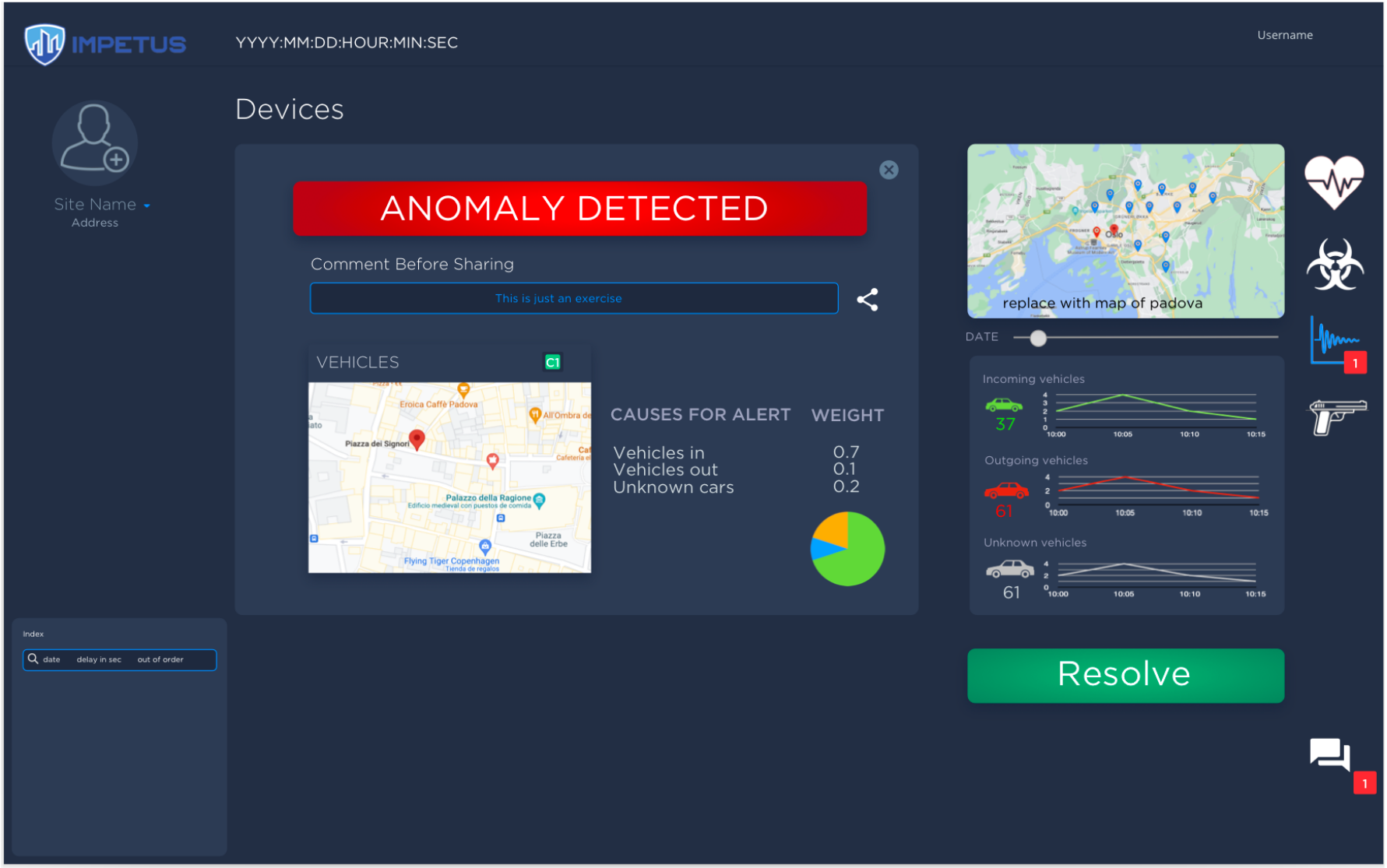

Figure 20. PTI Padova for vehicles

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 21 and Figure 22 below show the tool in idle mode, i.e., when no alert has been detected.

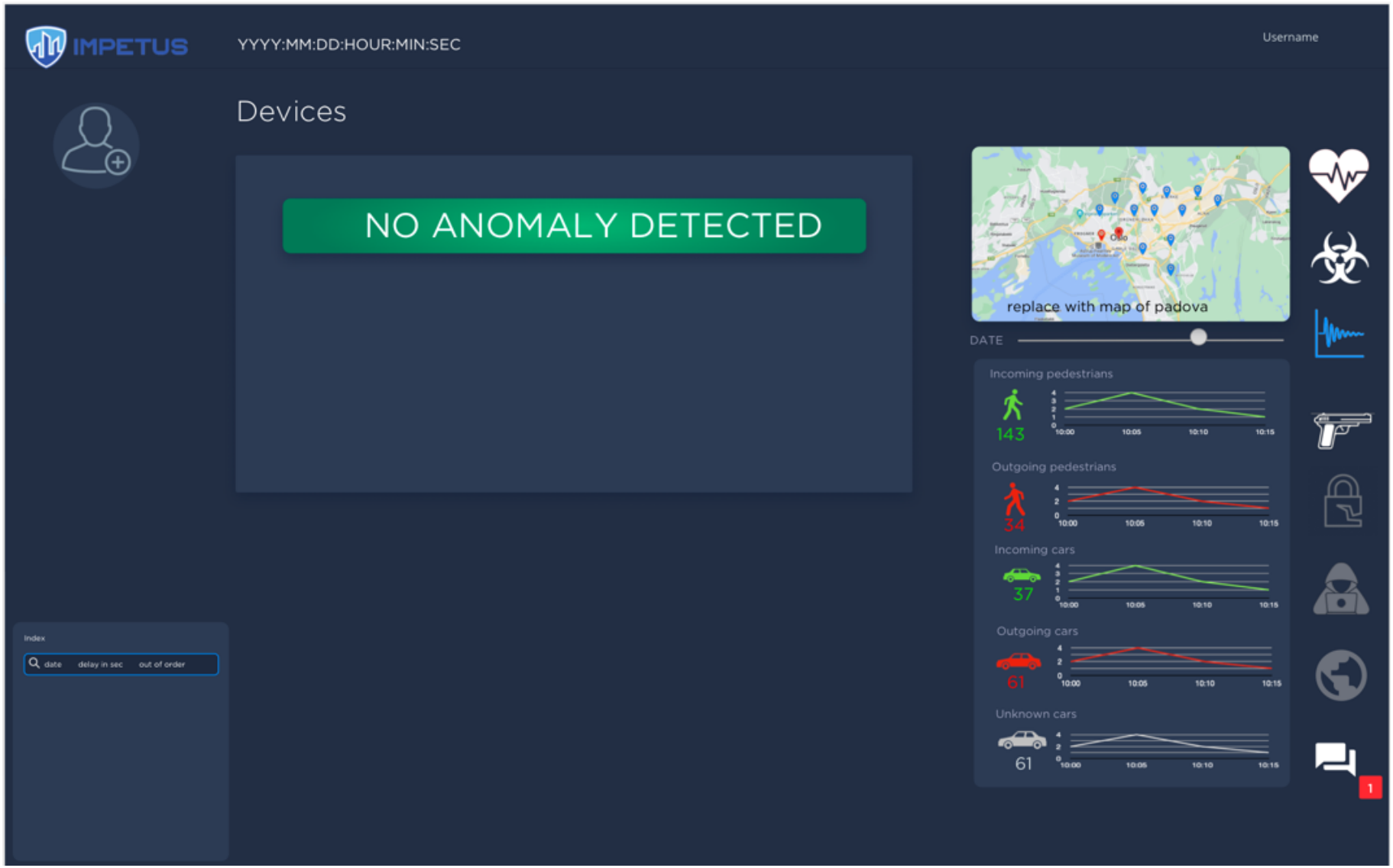

Figure 21. PTI for Padova in idle mode

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.

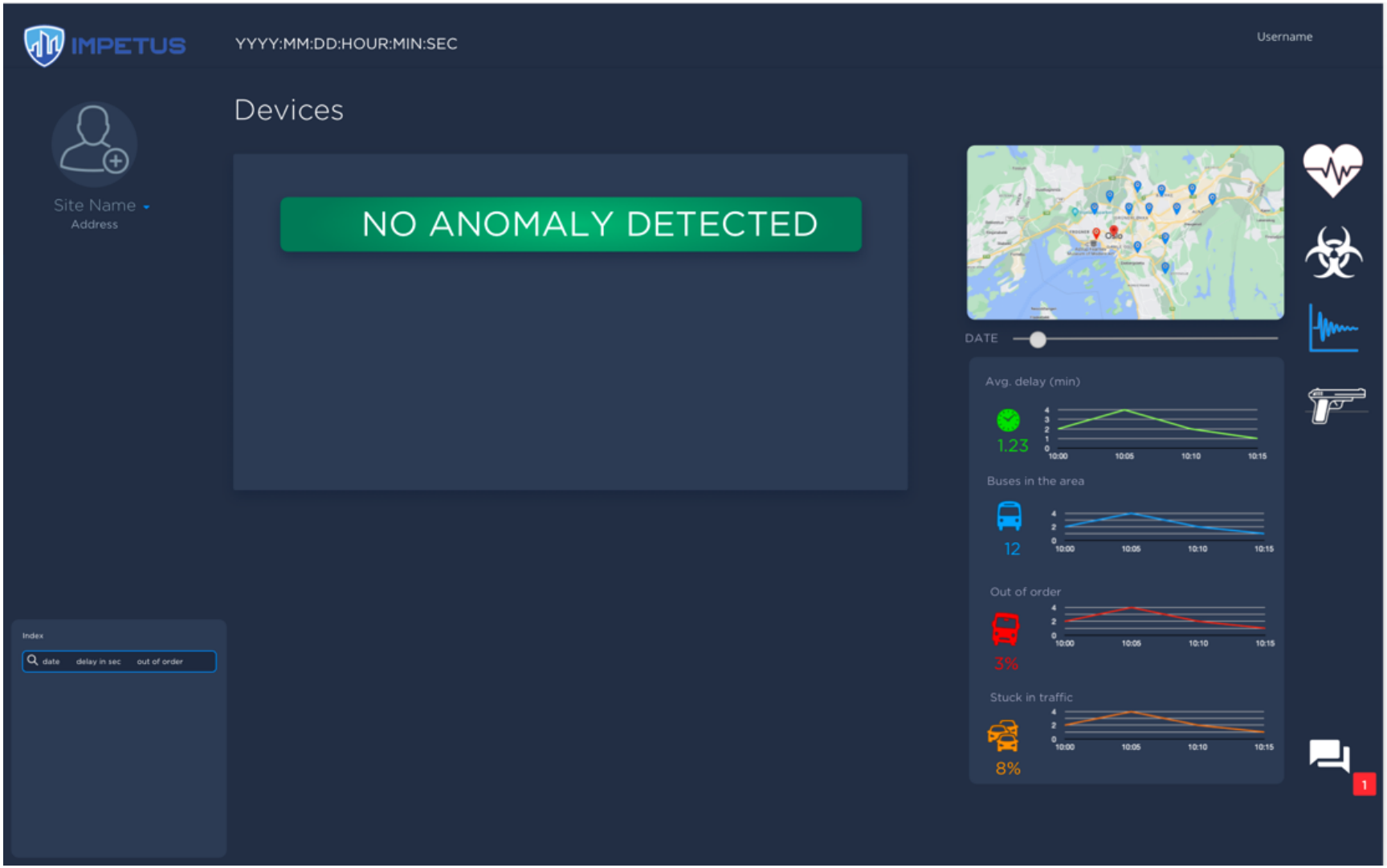

Figure 22. PTI for Oslo in idle mode

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.

3.6.1.3 Physical Threat Response Optimization (PTRO)

The PTRO provides a number of evacuation simulations from a number of public places relevant to the cities. The simulations take into account a wide arrange of factors (exits, entrances, fire danger, armed gunman, traffic…) and provide guidance to the SOC Operators as to what the most efficient egression strategies are for a number of given scenarios.

Clicking on one of the listed simulations automatically opens up a preview pop-up of the document containing a list of action to be taken or considered (Figure 23).

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.

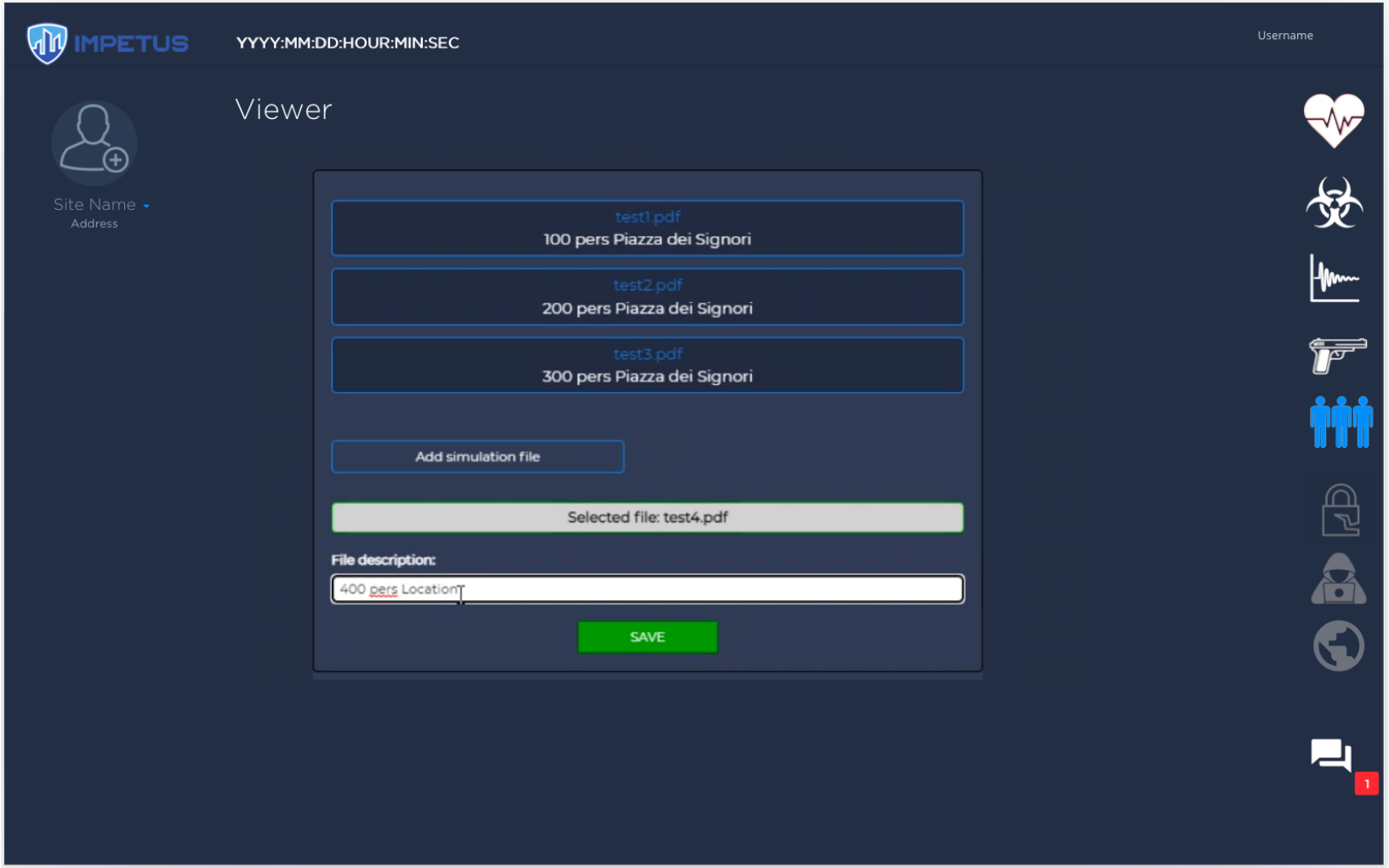

Figure 23. PTRO List of simulations

3.6.1.4 Bacterial Risk Detection (BRD) 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.

When the BRD tool detects an abnormal bacterial level in a space, sends the alarm to the SOC Operator telling them what the specific value concentration is as an absolute number and in a chart to be able to monitor the evolution and how high above the threshold it has climbed. It also provides the timestamp from when the latest data was analysed and when the next one is going to be, along with the location coordinates of the affected area and a list of immediate actions to be implemented as initial countermeasures. Figure 24 and Figure 25 show the tool in alert mode and in idle mode.

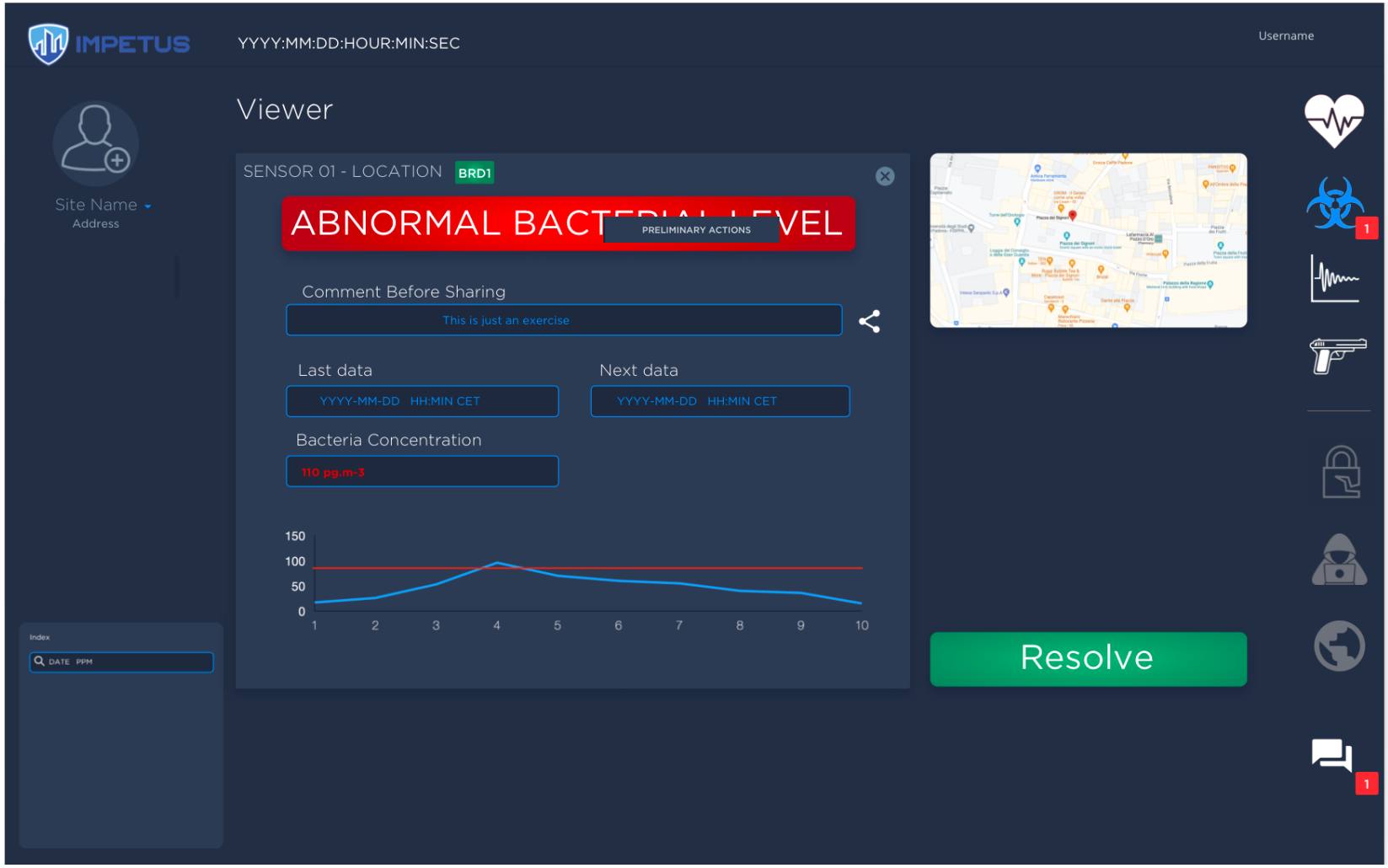

Figure 24. BRD Alert

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 25. BRD idle mode

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 system also notifies the SOC Operator when a specific sensor is undergoing maintenance (Figure 26) so they can be aware of the short periods during which the sensor is down.

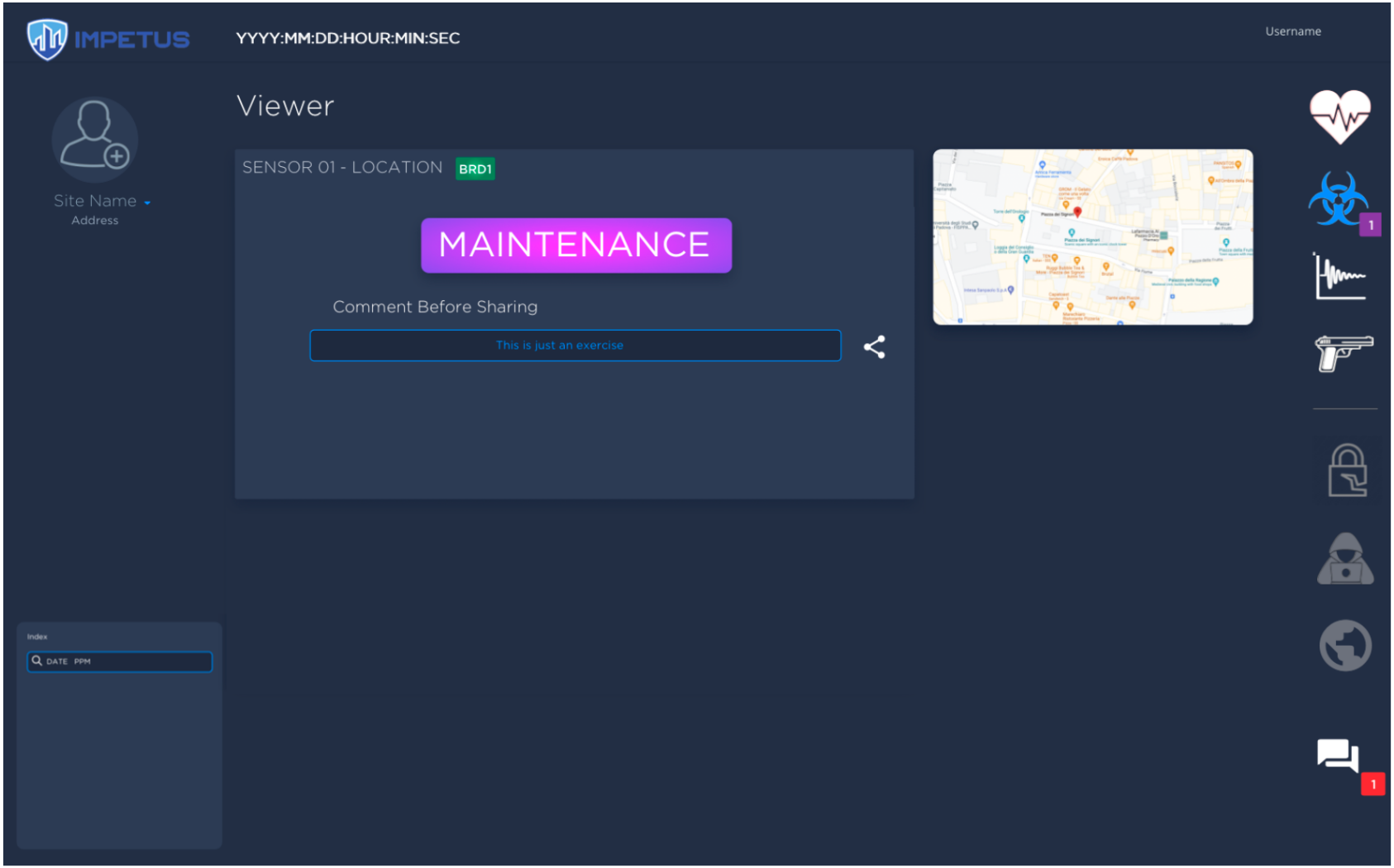

Figure 26. BRD maintenance notification

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.

3.6.2 Primary profile: IT Specialist

3.6.2.1 Cyber Threats Mapping (CTM) Tool

The CTM tool operates in a two-step process. First, the end-user launches a scan of their whole system using the Nessus platform. This scan can be accessed directly from IMPETUS as Figure 27 shows. The scan results in a file that is automatically downloaded to the end user's PC.

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.

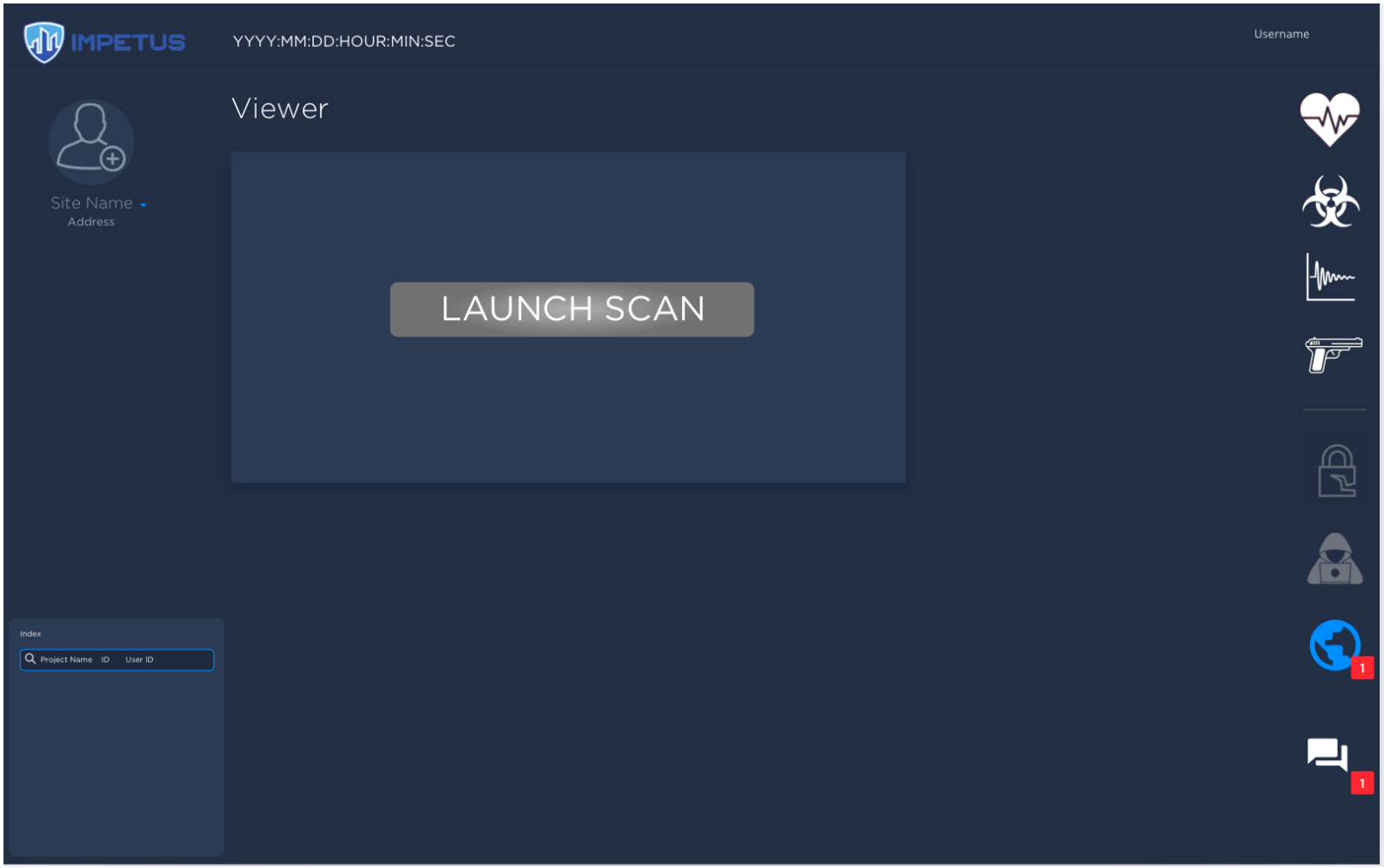

Figure 27. Launch Nessus scan

Secondly, this file is uploaded into the CTM tool, which runs an additional analysis and alerts the end user of any anomalies detected in the system are detected. The CTM tool provides through the IMPETUS platform a summary of the anomaly (Figure 28), listing what type of vulnerability it has identified, where it is located within the system, its level of criticality (immediately exploitable or at risk of being exploitable) and the suggested countermeasures to solve or mitigate 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.

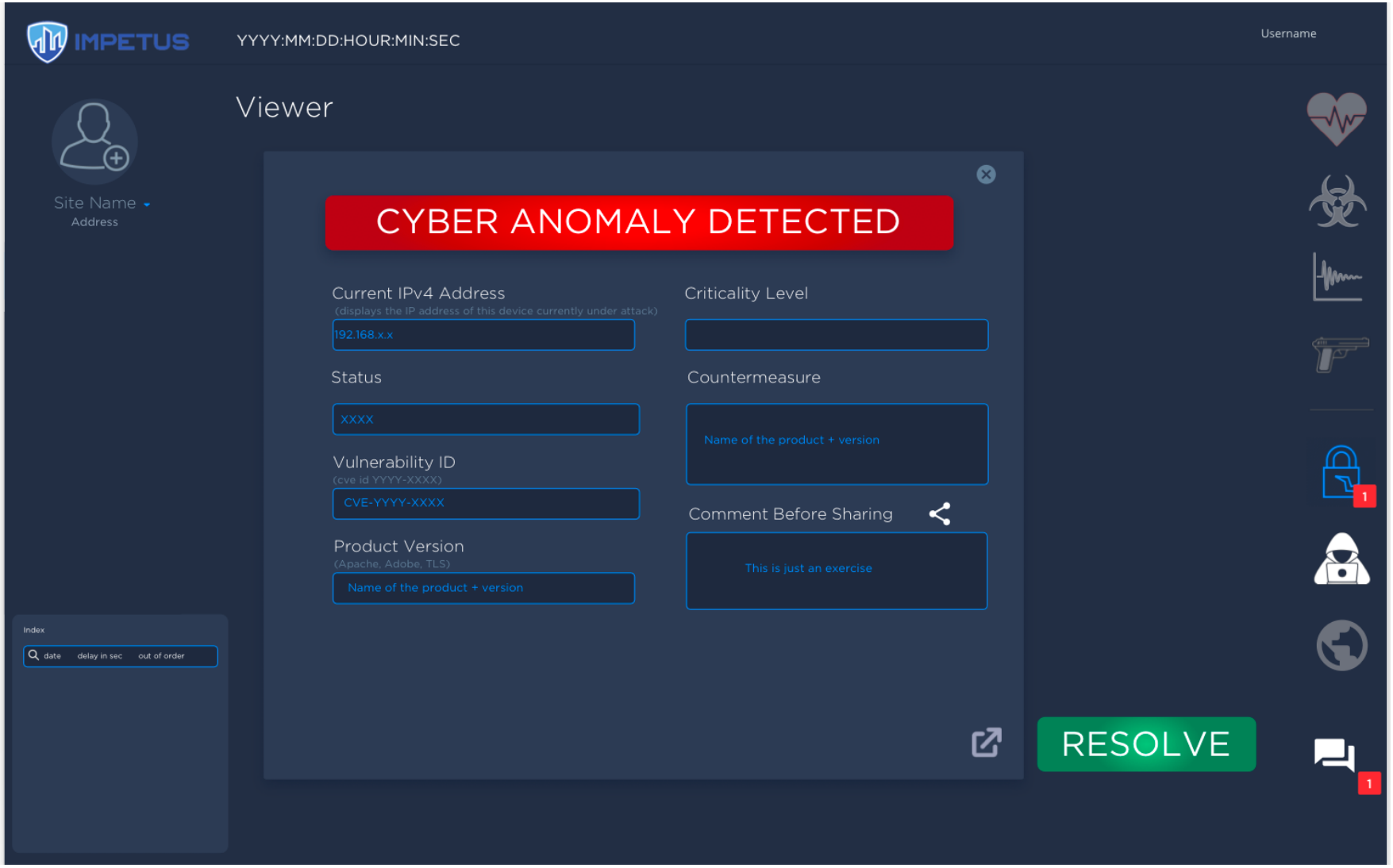

Figure 28. CTM alert notification

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.

3.6.2.2 Cyber Threats Intelligence (CTI) Tool

The CTI tool monitors the dark web and puts in front of the IT Specialists a list of the threats that are being discussed and can potentially expose the network and systems of the municipality. Even though the end user can specify what type of alerts they want to receive, the reality remains that the number of alerts received can be high to the point of becoming distracting and even disruptive to their usual workflow if they are notified about each one individually. Moreover, IT Specialists have and need more time to assess, treat and resolve an alert than SOC Operators do, for the problems they represent are different in nature. For these 2 reasons, it was deemed preferable that IT Specialists receive a notification called “new” when the CTI tool detects new threats, which are listed as “untreated” in the Cyber Sixgill proprietary platform.

The complete details for each alert, along with the possibility to self-assign or assign an alert to an IT specialist and check/mark each alert as “untreated”, “in treatment” or “resolved”, are features that the Cyber Sixgill platform already provides. Incorporating these features as well into the IMPETUS platform would be redundant. The preferred option was to show in IMPETUS the list of “untreated” and “in treatment” threats. Figure 29 shows how this is represented.

The alerts are divided by urgency (imminent and emerging) and by type (brand protection, compromised accounts, DDoS attack, data leak…). As it can be seen in Figure 29, the number for each category appear either in red or in grey, and they indicate the total number per category of “open alerts”. Alerts with the status “untreated” and “in treatment” are considered “open alerts”. If the number is in red and accompanied by the notification “NEW”, it tells the user they have new “untreated” alerts in the Cyber Sixgill platform. If the number is in grey, it indicates how many “in treatment” alerts they have for each category.

The number for a category change from red to grey when the user clicks on the external link icon () and updates the status from “untreated” to “in treatment” for those alerts in the Cyber Sixgill platform. This way, end users are always aware of how many “open alerts” they have at any given time and how many new ones have appeared since the last time they checked.

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.

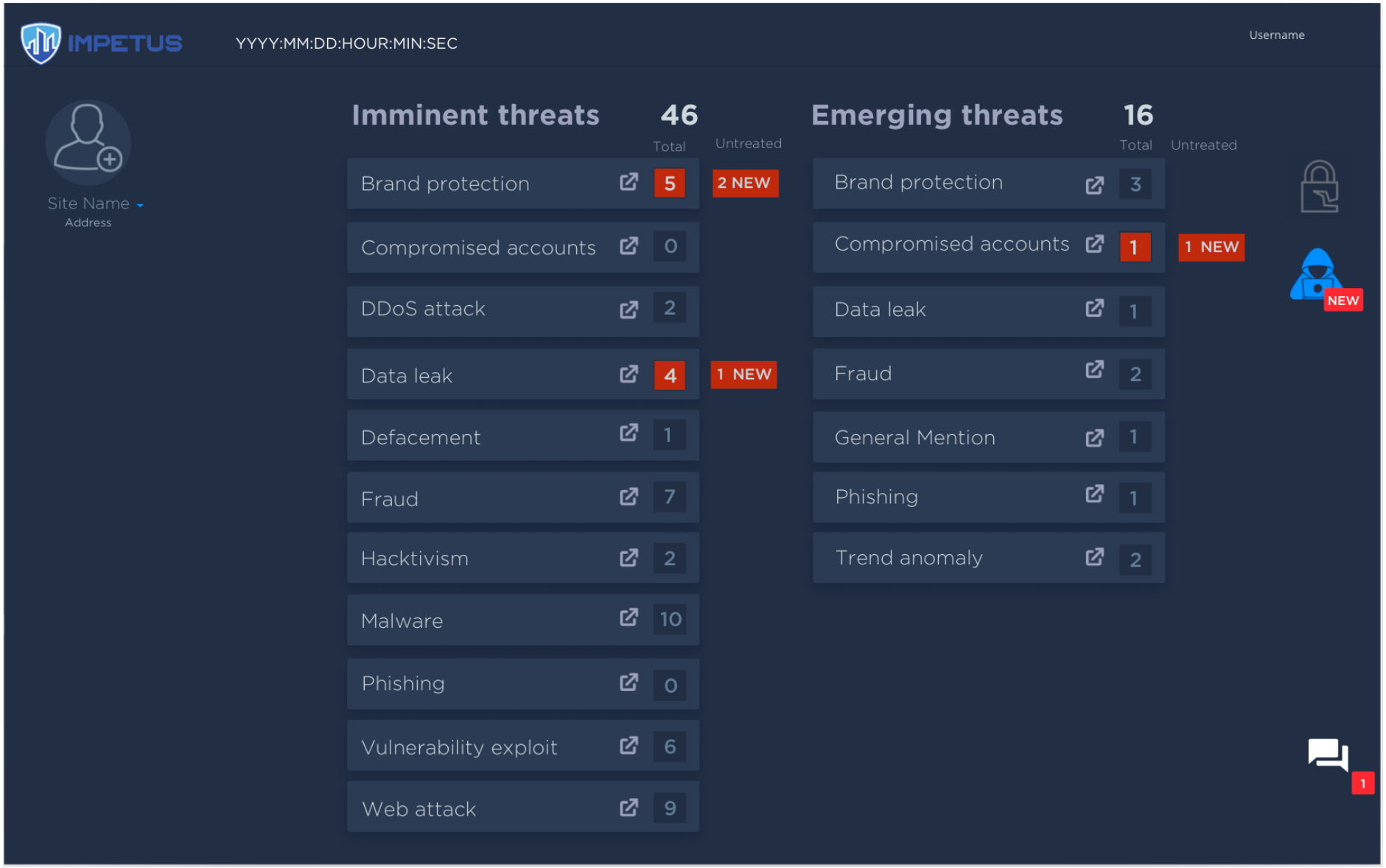

Figure 29. CTI New "untreated" alerts list

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.

If all the alerts are marked as “in treatment”, the IMPETUS platform will show it as Figure 30 indicates below:

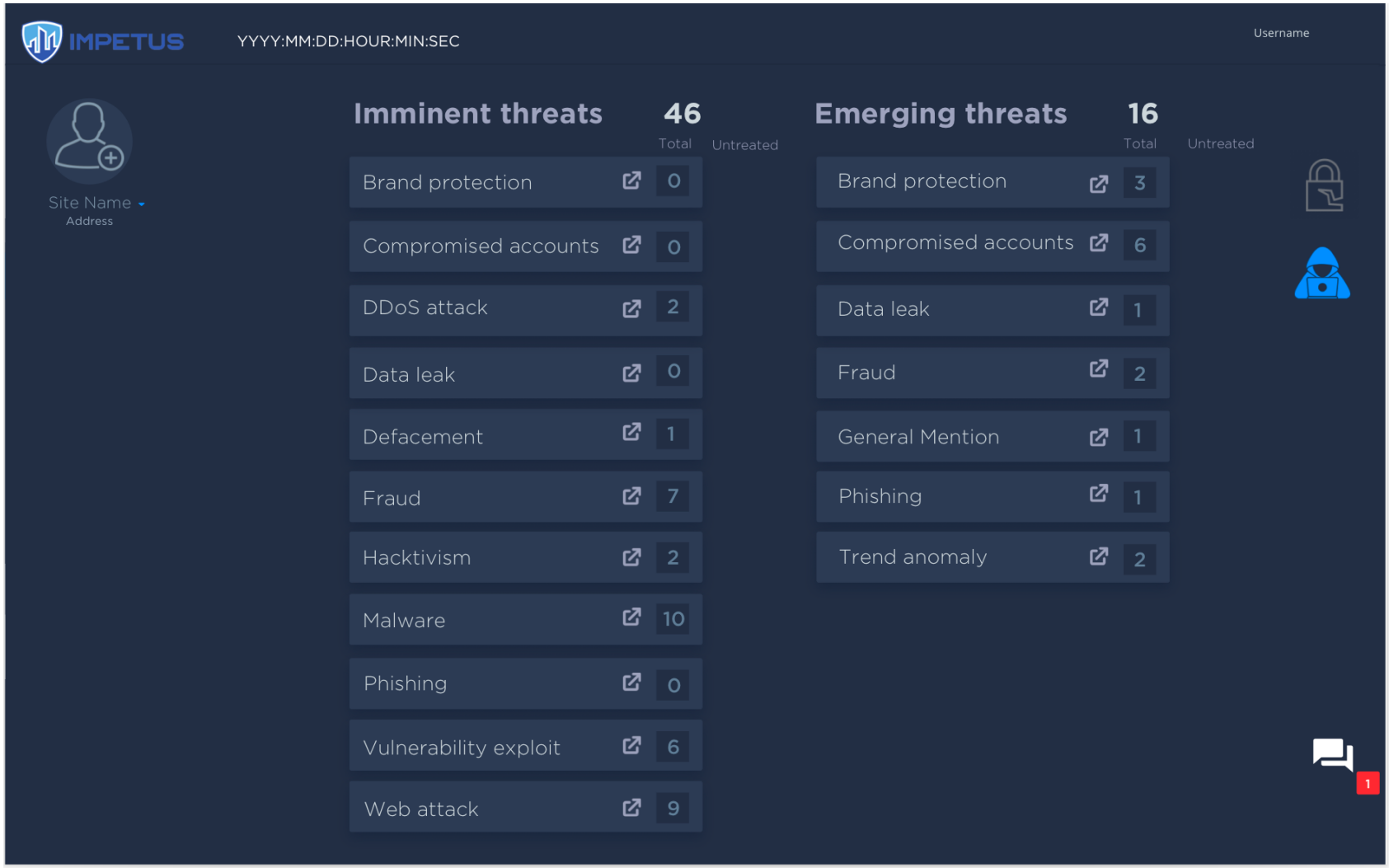

Figure 30. CTI List of "in treatment" alerts

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.

3.6.3 Primary profile: Intelligence Analysts

3.6.3.1 Social Media Detection (SMD) Tool

The first step to scan social media platforms and the open web to discover threats or insights into relevant topics is to set up a project searching for the chosen keywords. In order to do so, the end-user needs to access Spotlight, which they can do from the IMPETUS platform as shown in Figure 31.

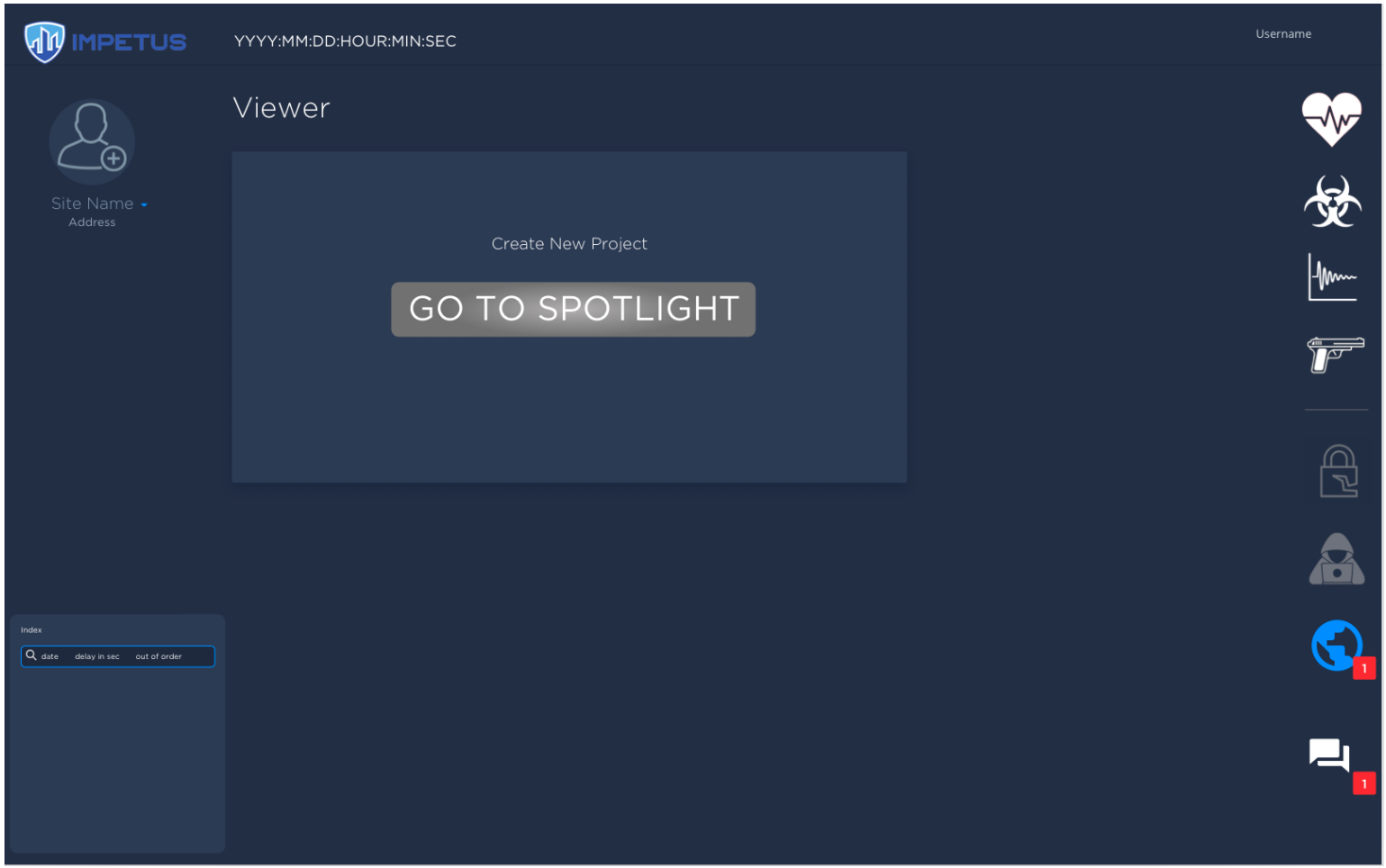

Figure 31. SMD Go to Spotlight

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 user is then redirected to the Spotlight interface where they will be able to log in automatically thanks to the authenticated ID protocol (Figure 32).

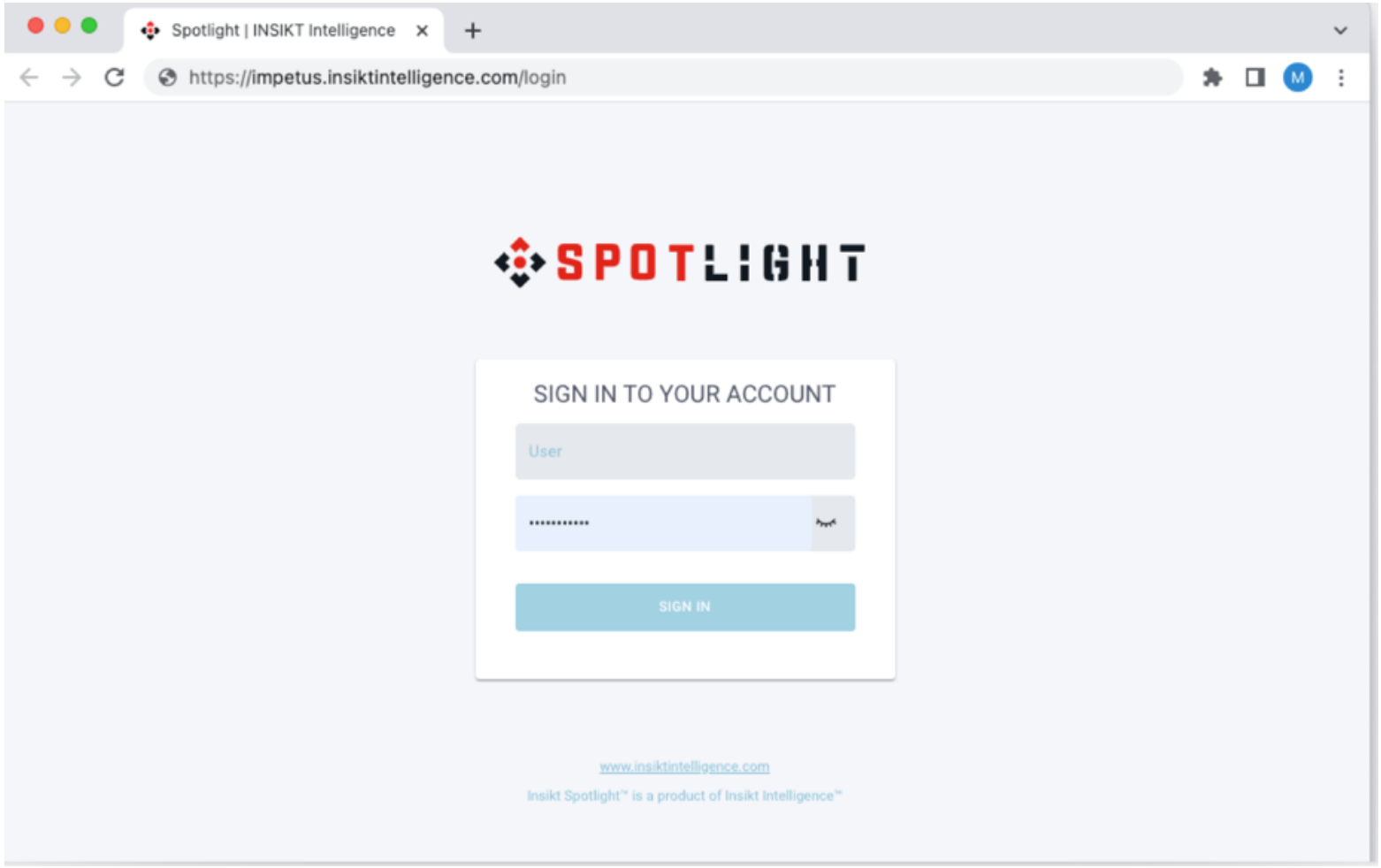

Figure 32. SMD Spotlight log in

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 end user will set up and launch the data acquisition and analysis in Spotlight and can direct their attention to other tasks while the project runs. Once the project is finished and the ready to be visualized, they will receive an alert through IMPETUS letting them know it is ready as seen in Figure 33.

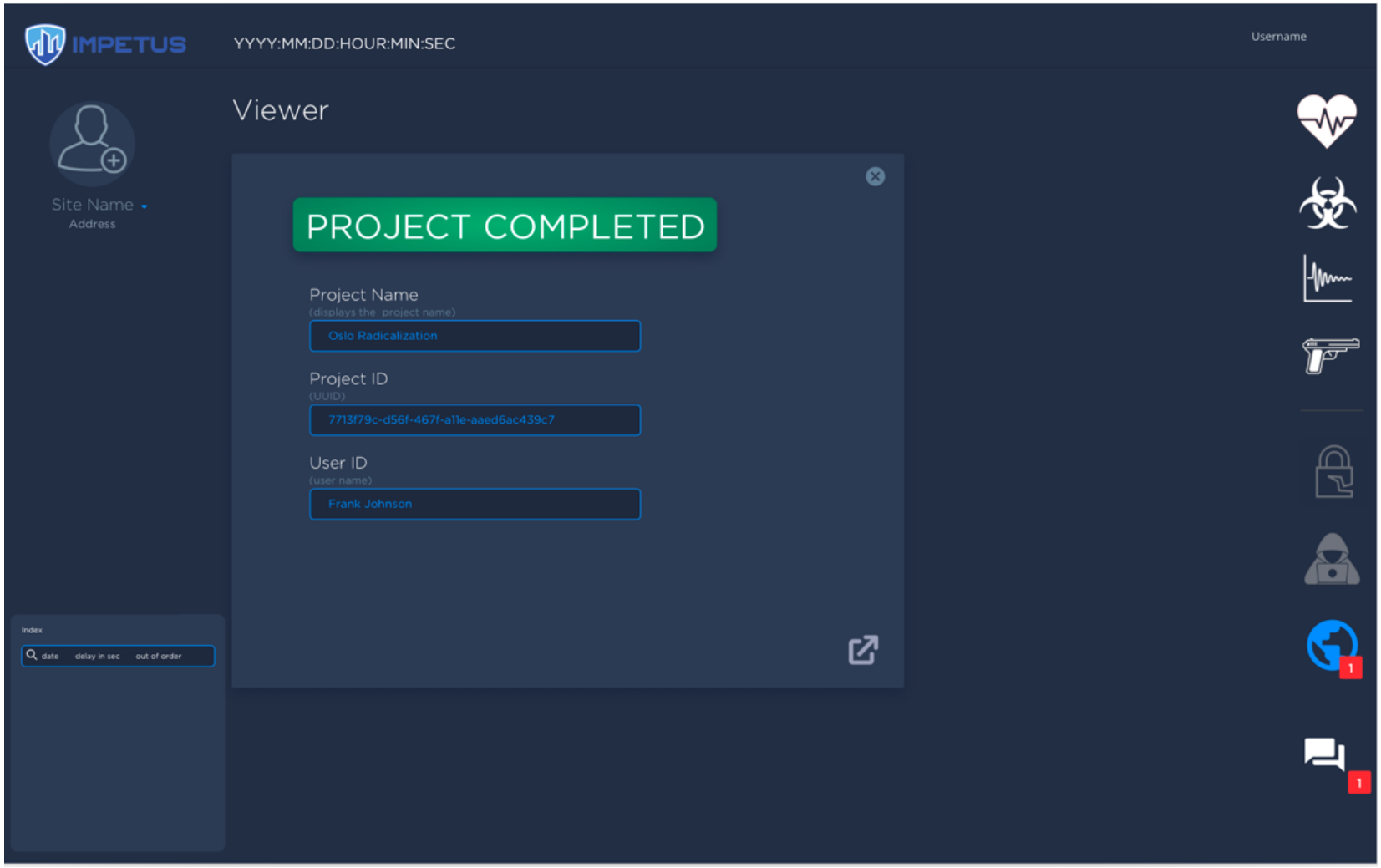

Figure 33. SMD Project completed alert

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.

If the system has encountered any sort of problem that has prevented the project from completing, the end user will receive an alert to this regard as shown in Figure 34. Even if highly unlikely, the goal is to avoid any situation where the end-user trusts the project is running and awaiting the results to later find out there has been a problem that made them waste precious time.

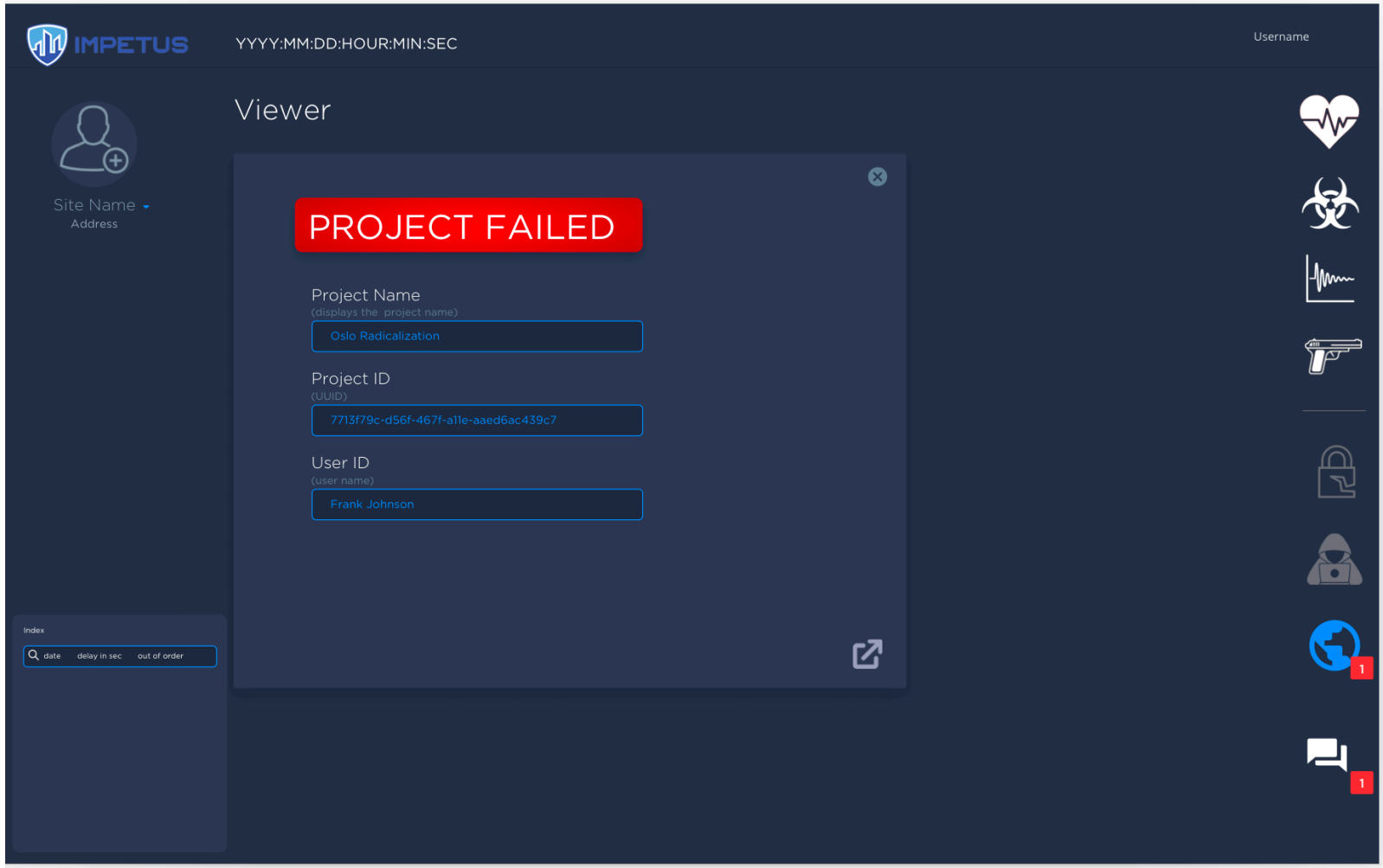

Figure 34. SMD Project failed alert

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.

After checking the results of the project, the end user, i.e., the intelligence specialist, can convey any relevant information to other profiles that need to be aware of the findings, for example SOC Operators or other stakeholders from the political sphere.

3.6.4 Main profile: Supervisors

Generally speaking, SOC and IT Supervisors need to have access to the same tools and functionalities as their teams to monitor situations and intervene when needed, either because an issue has been escalated their level or they deem it pertinent to intervene. The HCI tool helps them assess their team's emotional, mental and physical workload in a manner that increases Supervisors' situational awareness of their own teams, while other tools provide relevant information about the situations their teams are handling.

3.6.4.1 Human Computer Interaction (HCI) Tool

The SOC Operators and IT Specialists wear a headband during their shifts fitted with sensors tracking a number of variables that provide insight into their emotional, physical and mental wellbeing. When the workload in any of these 3 categories is considered high (out of low, medium, high), their supervisor gets an alert notifying them of the event (Figure 35). The supervisor can decide how best to intervene, or not intervene at all for it may be perfectly comprehensible that when handling an emergency, SOC Operators display increased levels of stress without that being a sign that they are underperforming. The alerts must naturally be put in context, and even though one single spike may not be consequential, they do provide the possibility to assess them over extended periods of time and make more global evaluations if needed. To access the full details of the alert, supervisors can access the HCI proprietary platform through the external link icon ().

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.

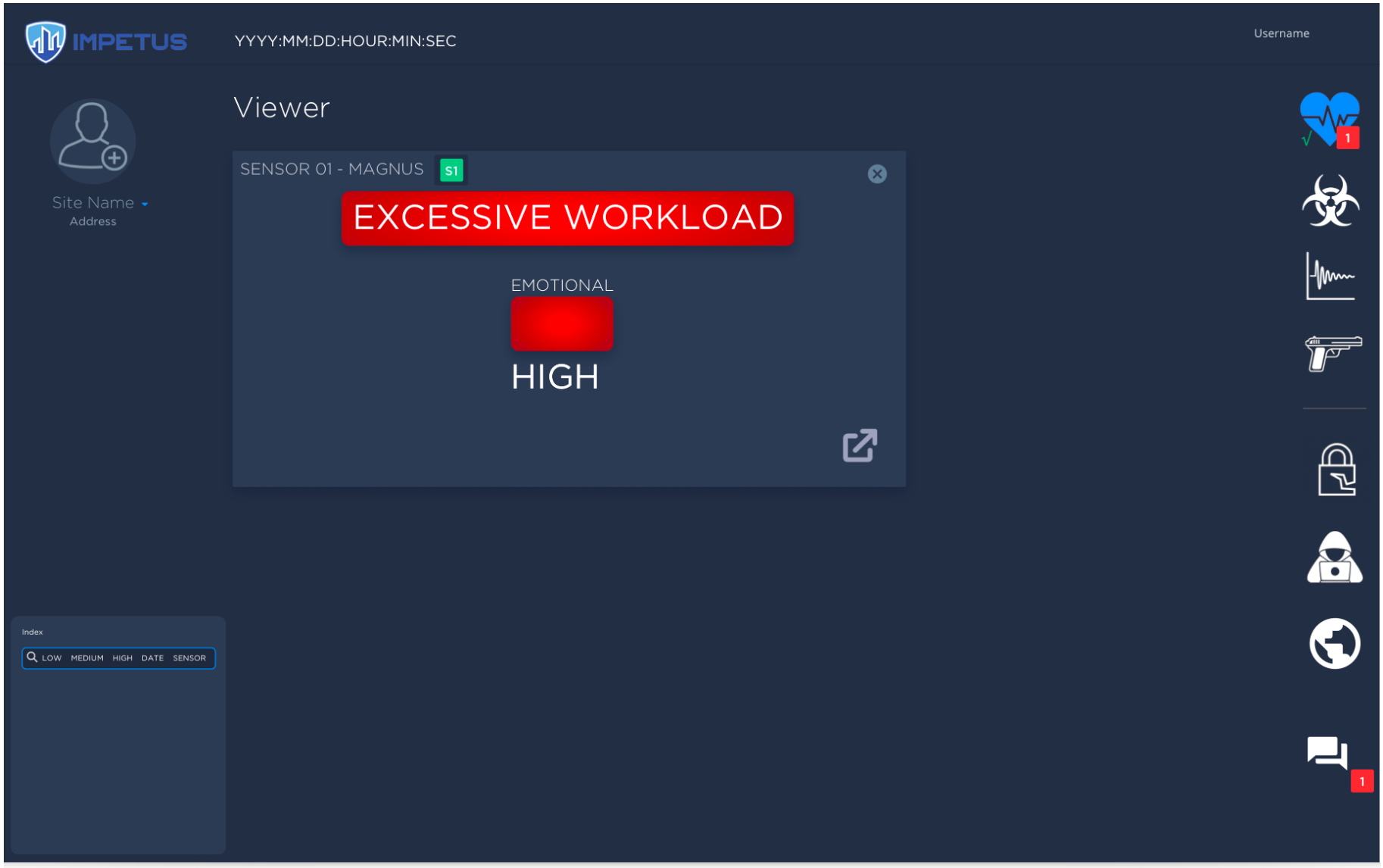

Figure 35. HCI notification of excessive workload

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 36 shows the HCI dashboard monitoring when there are no grounds to send an alert.

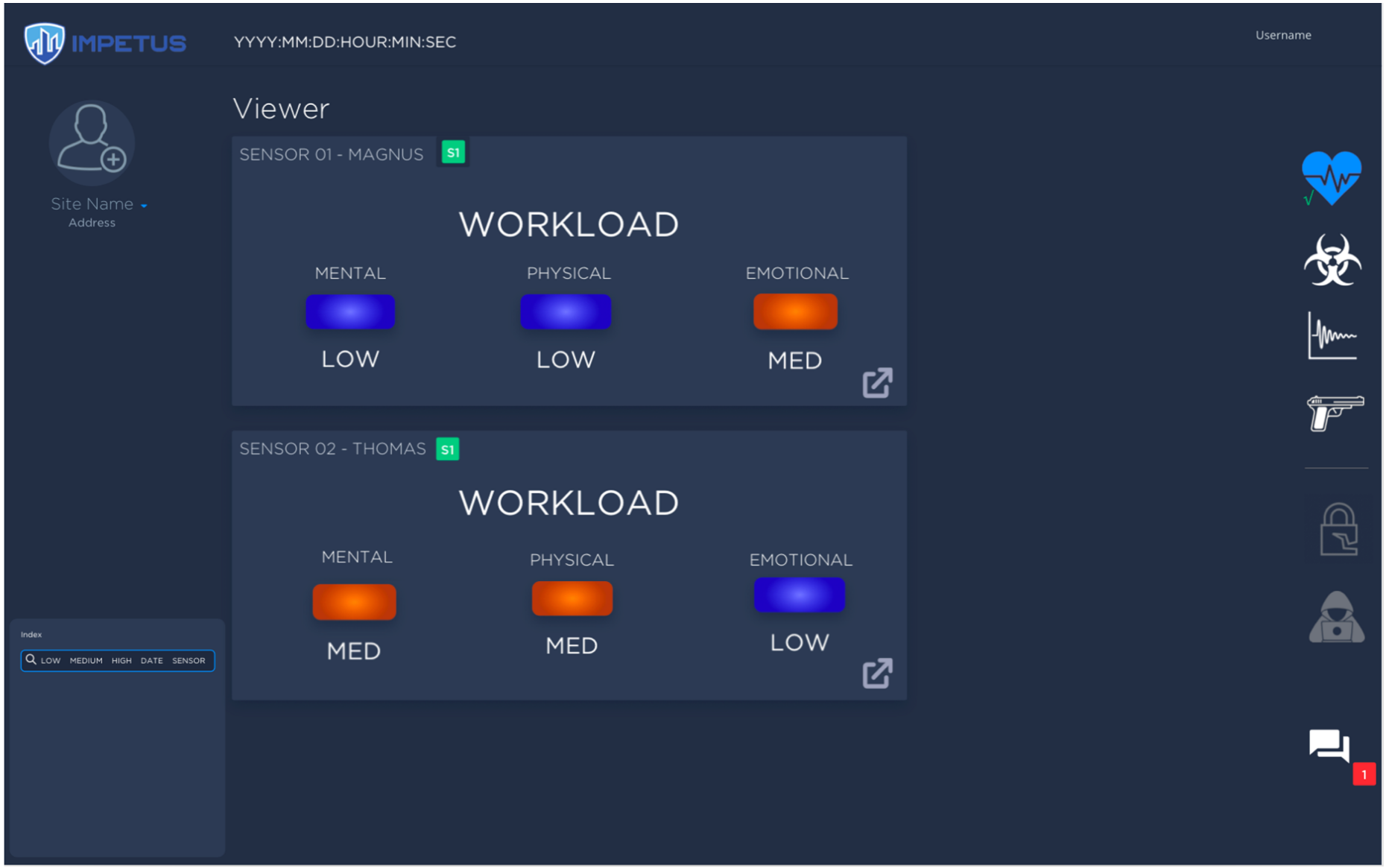

Figure 36. HCI Team monitoring

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 Big Data Visualizations

Big Data is understood as a collection of data that is huge in volume, containing different types of information and growing exponentially with time, so much so that traditional data management tools can store it or process it efficiently.

From all the tools in the IMPETUS tool set, 3 handle big data as such, namely PTI, CTI and SMD. Abiding by the principle of not duplicating information in the IMPETUS UI that is already accessible on the proprietary external tools' UI, in the case of SMD (Figure 37) and CTI (Figure 38) and, detailed big data visualizations have been kept in these external UIs, whereas the IMPETUS UI incorporates, in the form of alarms, the highlights that would warrant specifically consulting the big data visualization.

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.

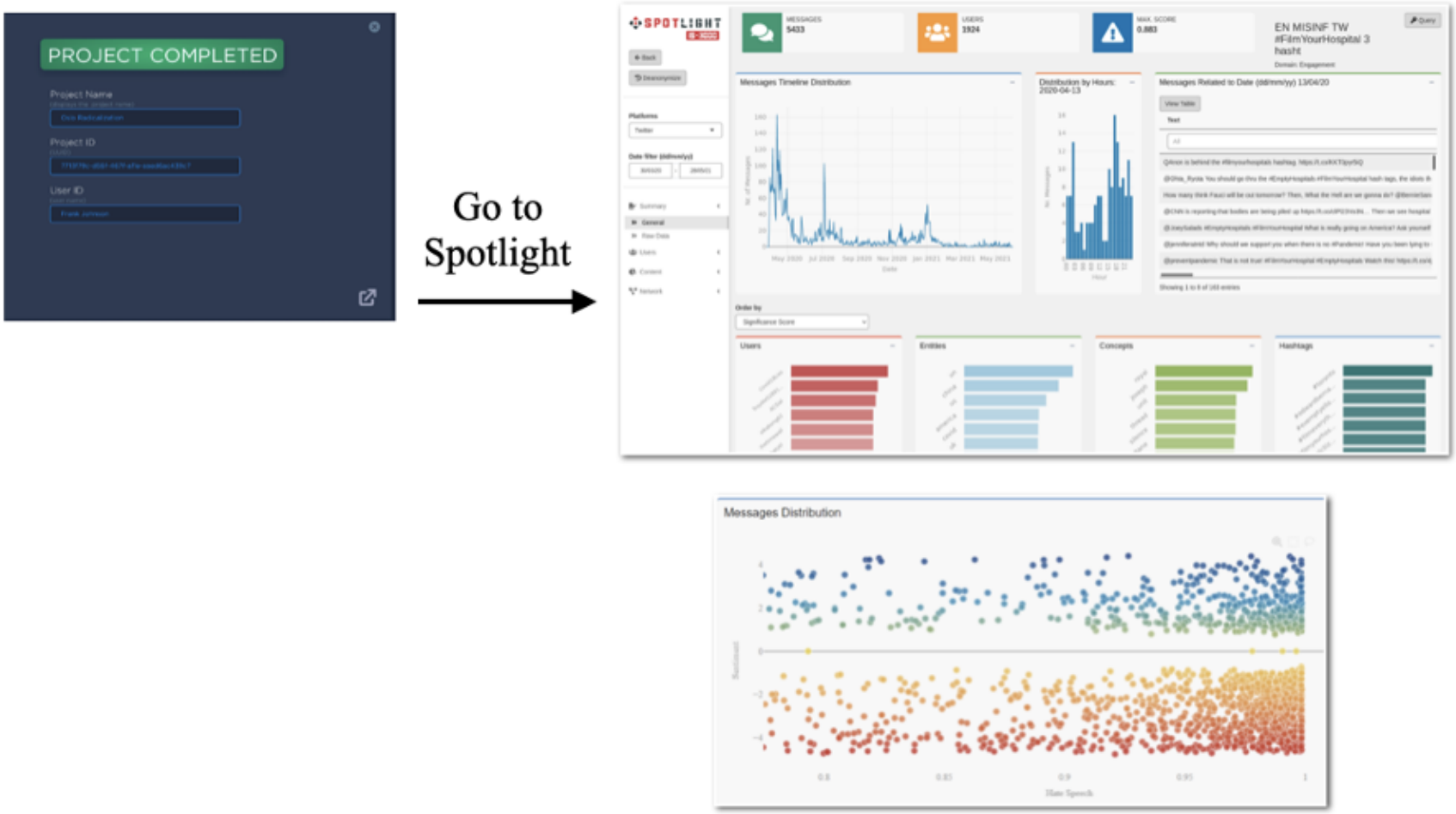

Figure 37. Example of SMD Big data visualization

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.

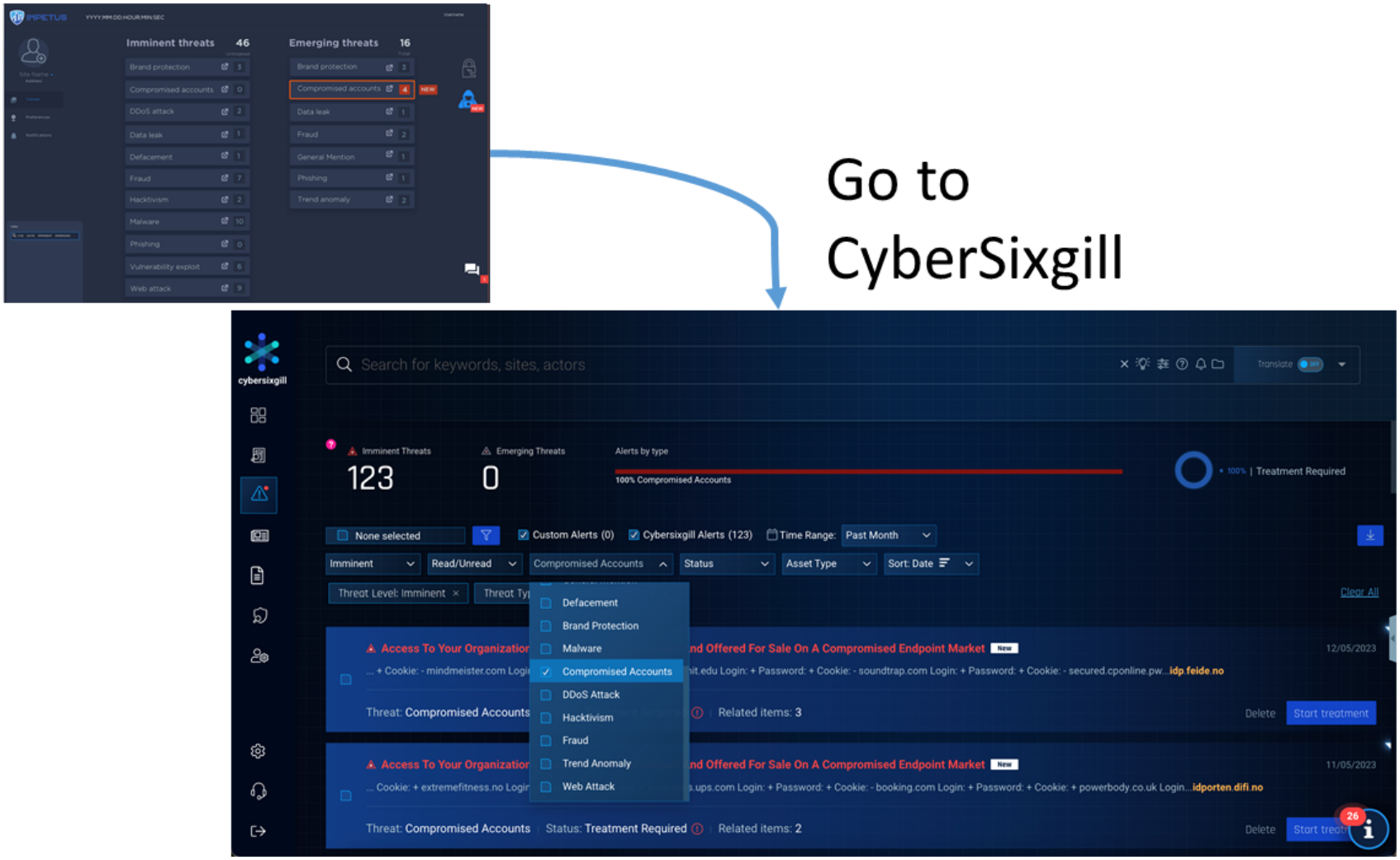

Figure 38. Example of CTI Big data visualization

Both SMD and CTI allow in their proprietary UI different ways to filter, navigate and visualize data, as the functionalities highlighted in green exemplify: in the case of SMD, data can be visualized and filtered by date, level of significance, hate speech level, by specific concepts, entities, key ideas, hashtags, etc., and

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 bubble graphs permit different visualization configurations of the variables displayed in each axis and the colour legend. In the case of CTI, threats can be filtered and visualized according to their status, type, date, immediacy, etc. Both tools ensure that the same information can be accessible through different pathways so the end user can choose which one suits them best on every occasion.

The PTI case

When developing the UI for the PTI tool, which, contrary to the case of the SMD and CTI tool, did not have a pre-existing UI, one of the main challenges to solve was the concept of interpretability. Interpretability refers to how readable, intuitive and coherent the outputs of the big data visualization are or, simply put, if these outputs are understandable enough to be truly useful for the end user. Naturally, this determination is directly correlated with the end user profile these outputs are intended for, i.e., their level of knowledge, field of expertise and expectations. In the case of the IMPETUS, it was imperative to present data in a manner that was suitable for non-technical profiles who are not (and do not need to be) proficient in algorithmic rules or extensive data series interpretation.

Even though the data sets and variables gathered from Oslo and Padova are different (static sensors measuring traffic and pedestrian flows across points of interest in the case of Padova, and data gathered from the fleet of public transport buses in transit in the case of Oslo), the rationale behind the way alerts are displayed is the same for both cases: to provide the “core” information about the anomaly (elements outlined in yellow in Figures 39 & 40), to put it in as much context as possible (elements shaded in yellow in Figures 39 & 40) and to rely on friendly self-explanatory images and colour coding whenever possible (icons for the variables, colour matching).

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.

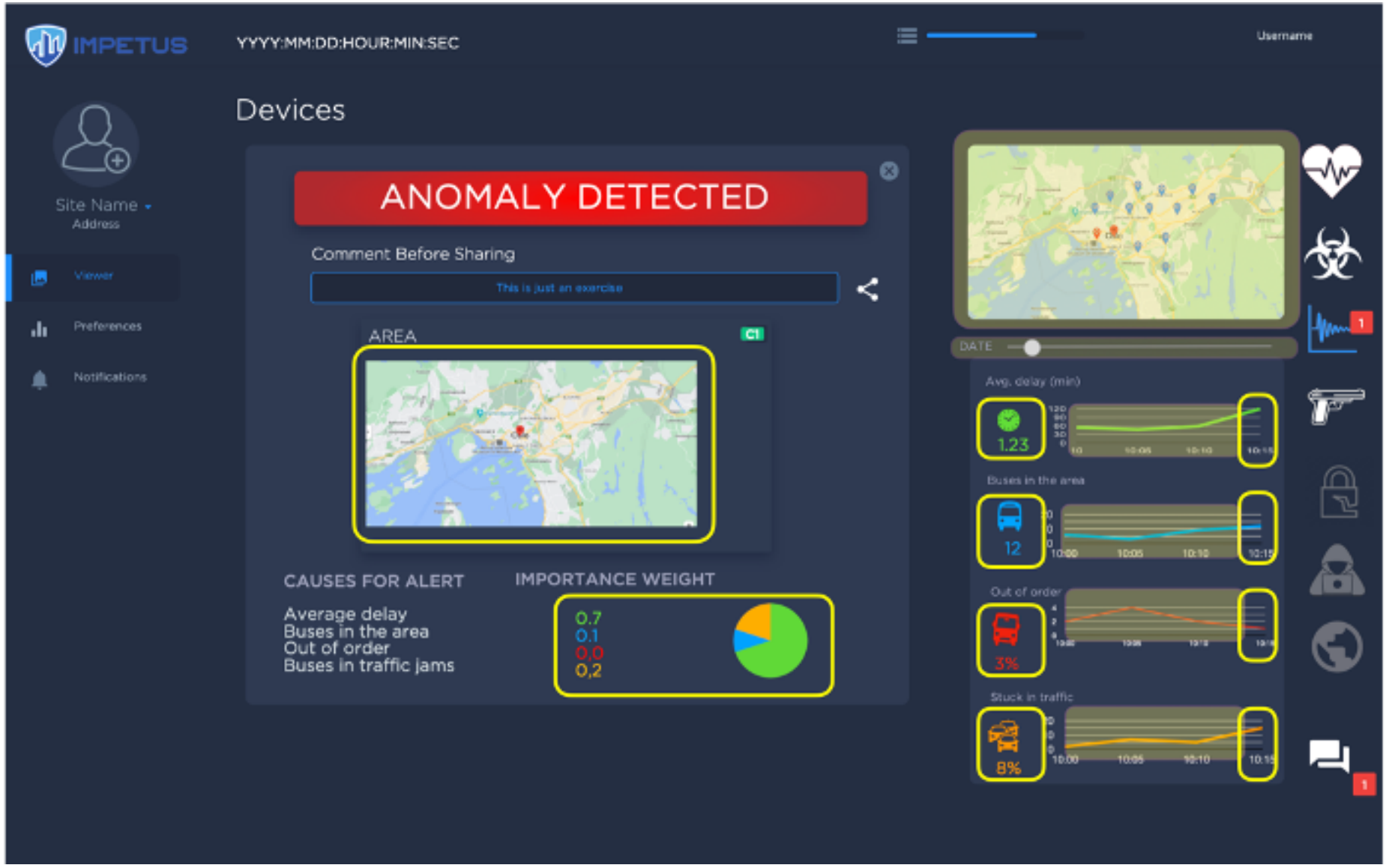

Figure 39. Oslo PTI alert

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.

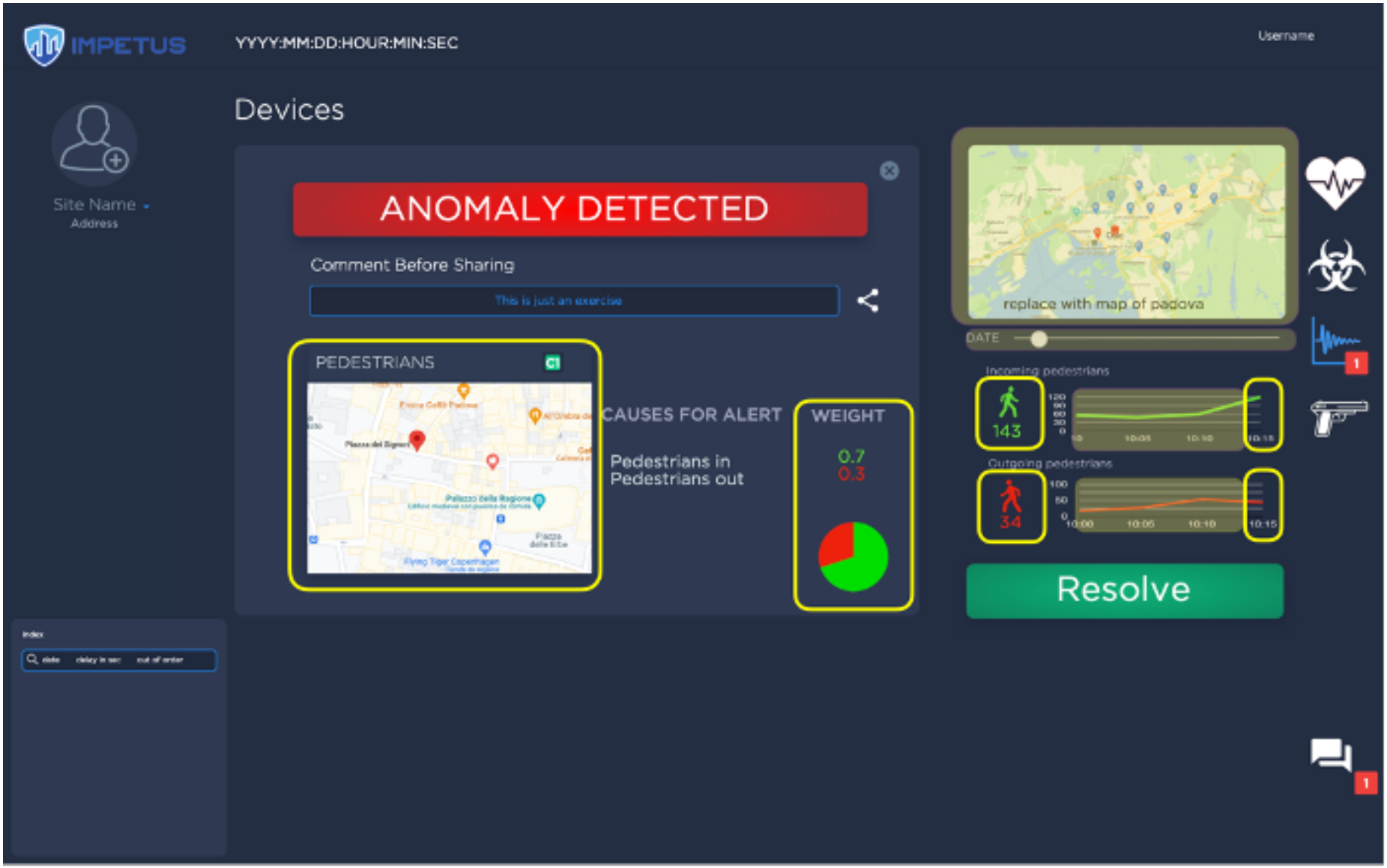

Figure 40. Padova Pedestrians PTI alert

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 elements outlined in yellow in Figures 38 and 39 represent the data points that conform the anomaly alert in itself, namely the values featured below each icon, those same values represented as the most recent point in a time graph, the time stamp in the graph, the geolocation and how much has each variable contributed to the “anomaly declaration”. These latter importance weights are shown numerically with a decimal number from 0 to1 (the sum of all variables’ weights needs to equal *1*) and with a pie chart with the same values represented as sections of a pie for further clarification.

Conversely, the elements shaded in yellow are not strictly part of the alert per se but still provide contextual relevant information to the end user: the map on the top right (see Figures 38 & 39) shows if there are any additional anomalies detected at the same time in other areas of the city; the timeline graphs underneath the map allow the SOC operator to put each absolute value the context of a time series and visualize the evolution of each variable in the period right before the alert was triggered. Furthermore, the date slider between the map and the graph lets the user go back in time and review past events which may provide additional insight about potential repetitive patterns, for instance.

The incorporation of these contextual data points around each alert is particularly noteworthy because, in the case of the PTI tool, there are no false positives. Every anomaly detected is truly a deviation of standard parameters; however, by no means every anomaly constitutes an actual emergency. The goal of providing context for each anomaly is to offer to the SOC operator a holistic view so that it becomes easier for them to ascertain the true transcendence of that set of abnormal conditions. The visualization strategies implemented let them know, for instance, exactly what colleague on the field to contact thanks to the geolocation of the alert; or when a spike in pedestrian inflow to Piazza di Signori is detected, for example, to monitor in real time whether it resolves itself organically after 5 minutes or if, on the contrary, alerts of increased inflow are sustained over time, continuously increasing in value and warrant further attention or even intervention.

Additionally, this holistic approach can also assist SOC operators, as the humans the loop, to choose what sensitivity level of the PTI tool (low, medium, high) detects more accurately the types of alerts that can potentially constitute an emergency or a situation to monitor closely.

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 Future Work

The IMPETUS UI has been developed keeping the needs of the end users in mind and following their first-hand indications regarding their requirements; thus, the user interfaces correspond to a fairly mature and operational interface. However, it is possible that during the validation exercises adjustments are identified that can further improve the user experience and the robustness of the platform as a whole. A key component of the live demonstrations will be to gather further input from stakeholders (operators, evaluators and expert observers) in 2 rounds, firstly in Oslo (August 2022) and secondly in Padova (October 2022). If potential improvements are indeed recognized, they will be presented in the deliverables pertaining to WP2 and/or WP7 and the user interface updated accordingly.

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
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

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.