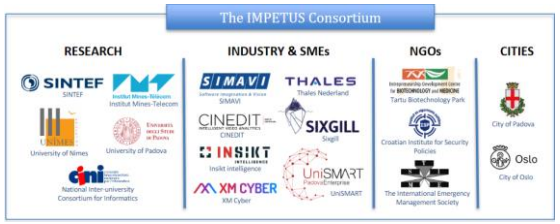


TIEMS – CBI Webinar on the IMPETUS Project

1. **Joe Gorman**, *SINTEF, Norway* - **IMPETUS Project overview and Expected Results**
2. **Jelena Radosevic**, *ISP, Croatia* - **IMPETUS Public Opinion Survey on Ethical Issues on Smart cities Technologies**
3. **Radu Popescu**, *SIMAVI, Romania* - **IMPETUS Platform - Integration of Tools**
4. **Joe Levy,** *CINEDIT, Switzerland* - **IMPETUS Weapon Detection Tool**
5. **Joaquin Luzon Tuells**, *INSIKT, Spain* - ***IMPETUS Social Media Threats Detection Tool***
6. **Osman Mohammad Ibrahim**, *City of Oslo, Norway* - ***IMPETUS Solutions Implementation in City of* Oslo**
7. **Sandro Bologna**, *TIEMS, Belgium* - ***IMPETUS - COSSEC Network***

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

IMPETUS

A research and innovation project addressing urban safety

IMPETUS

Intelligent **M**anagement of **P**rocesses,
Ethics and **T**echnology for **U**rban **S**afety

A Horizon 2020
Research and Innovation Project

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

IMPETUS: Intelligent Management of Processes, Ethics and Technology for Urban Safety

Key facts

- H2020 IA project
- Topic: SU-INFRA02-2019 Security for smart and safe cities, including for public spaces
- Total budget 9.3 M€, EC funding 7.9M€
- September 2020 – February 2023
- Overall goal: Improve the security of public spaces in smart cities

Consortium

RESEARCH

SINTEF

Institut Mines-Télécom

UNÎMES

Università degli Studi di Padova

cini consorzio interuniversitario nazionale per l'informatica

INDUSTRY & SMEs

SIMAVI Software Imagination & Vision

THALES

CINEDIT Intelligent Video Analytics

SIXGILL

INSIKT INTELLIGENCE

XM CYBER

UniSMART Fondazione Università di Padova

NGOs

Entrepreneurship Development Centre for BIOTECHNOLOGY and MEDICINE

ISP

TIEMS

CITIES

Commune di Padova

Oslo

… complemented by COSSEC:

Community of Safe and Secure Cities (extends involvement)

Contact info

www.impetus-project.eu

Project Coordinator: Joe Gorman, SINTEF Digital: joe.Gorman@sintef.no

COSSEC Manager: Sandro Bologna, TIEMS: s.bologna@infrastrutturecritiche.it

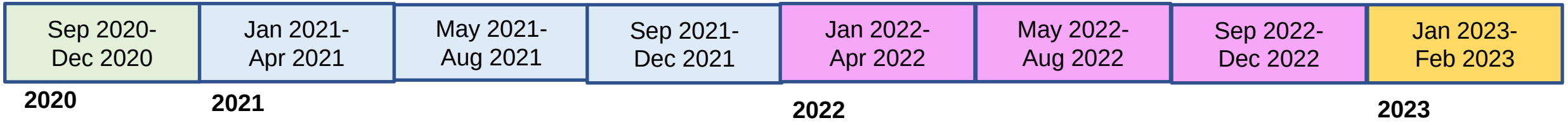
Dissemination manager: Snjezana Knezic, TIEMS: snjezana.knezic@gmail.co

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

WHEN will IMPETUS happen?

Challenging: 30-months duration

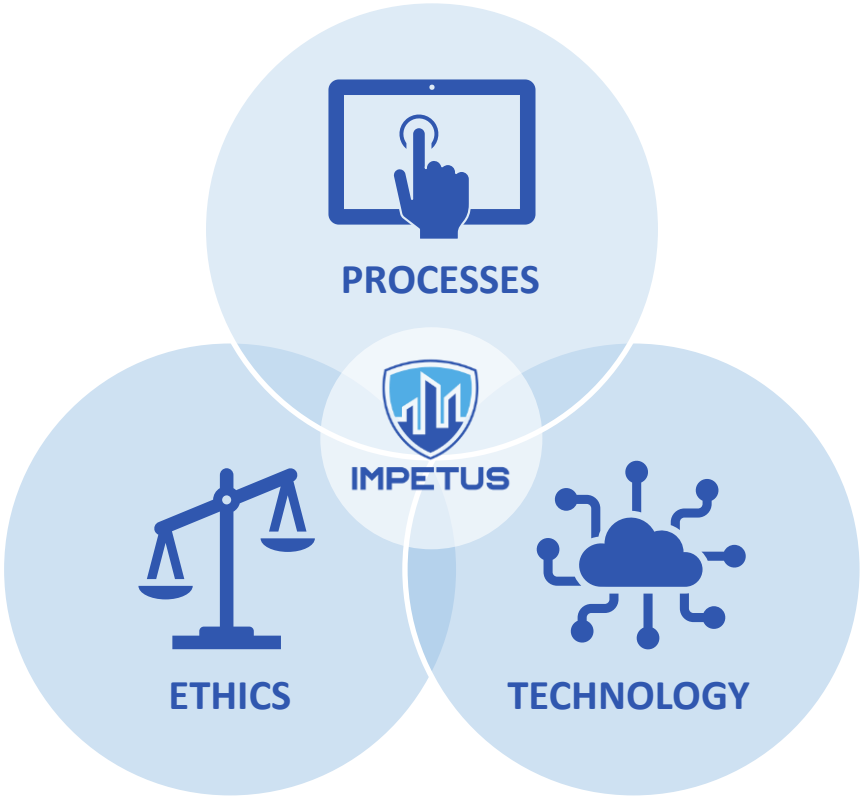
Today



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

WHY IMPETUS: Main objective

The IMPETUS intersection: integrating interdependent solutions and concerns



Improve the security of public spaces in smart cities

- Can advanced **technologies** improve the detection and management of security events?
- How will this affect **processes** used in day-to-day operations?
- How can **ethical** and legal issues be safeguarded and handled?

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

WHY do Smart Cities need IMPETUS?

Smart Cities

- High-tech grid of sensors (cameras, environmental sensors, traffic sensors, …)
- IoT (”Internet of Things”) – internet is everywhere – not least in everyone's pockets
- IT systems controlling critical infrastructure
- Advanced algorithms and AI (Artificial Intelligence) to help people make decisions

Efficient city administration

Enhanced situational awareness, especially in emergencies

Help authorities make sound decisions, fast

←Enhance

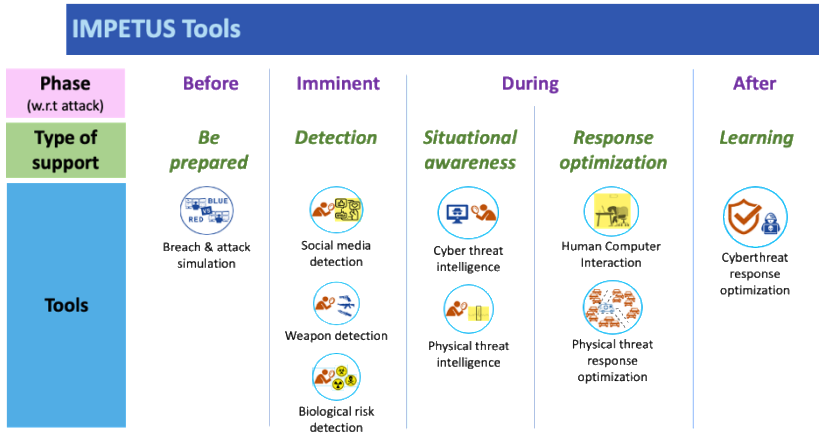
Combat→

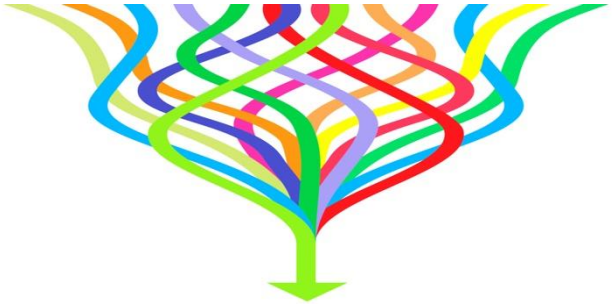
Increased “attack surface”- more vulnerabilities e.g. cyber attacks

Increased risk of unethical use of personal data

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

IMPETUS: Key Results





Integrating Platform

- Tools usable in single interface
- Tools can connect and share data

Practitioner's Guidelines

- Advice
- DOs and DON'Ts
- Reference information
- Training materials

Other projects

First adopters

Policy makers

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

IMPETUS Tools

Phase (w.r.t attack)	Before	Imminent	During		After
Type of support	*Be prepared*	*Detection*	*Situational awareness*	*Response optimization*	*Learning*
Tools	 Breach & attack simulation	 Social media detection  Weapon detection  Biological risk detection	 Cyber threat intelligence  Physical threat intelligence	 Human Computer Interaction  Physical threat response optimization	 Cyberthreat response optimization

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

WHERE and how will IMPETUS be validated?

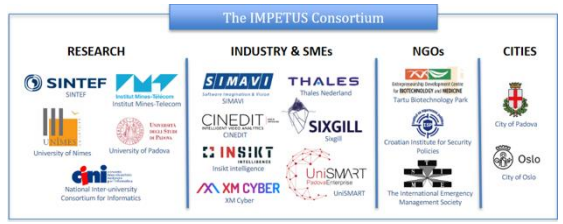
Validation pilots in two cities

- Phase 1: Technical and acceptance testing on non-live systems
- Phase 2: Data collection from live systems, for analysis but no intervention
- Phase 3: Live test with simulated physical and cyber attack

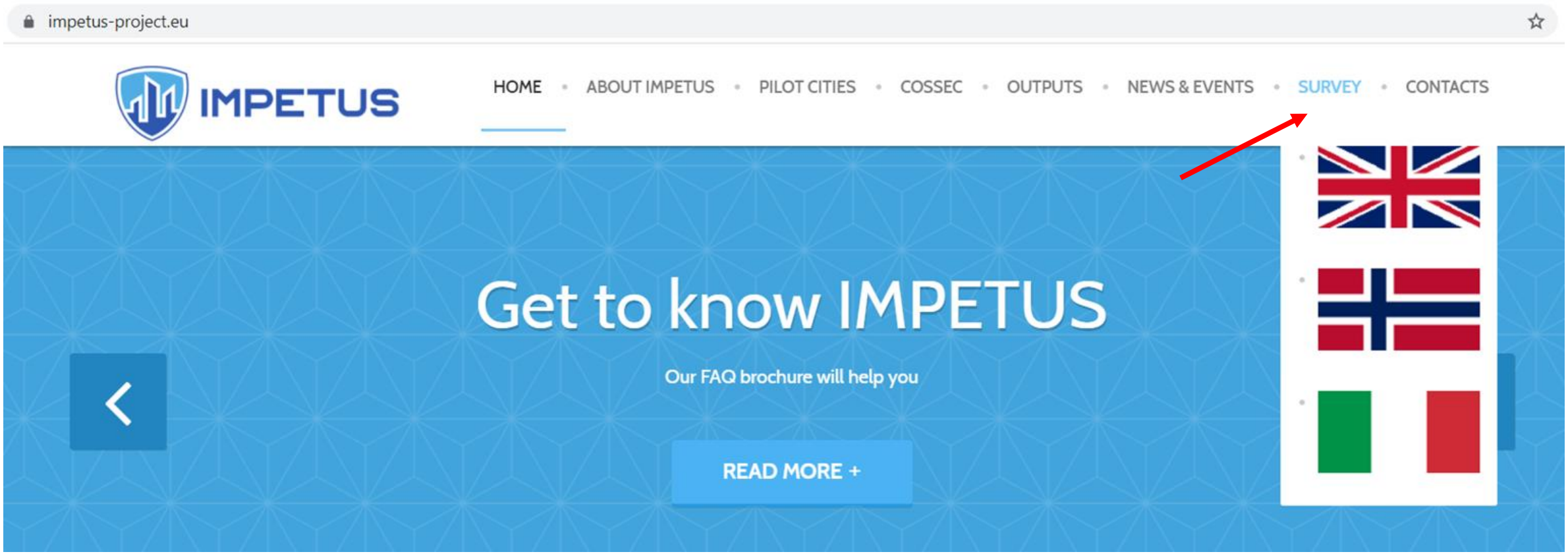
Oslo, Norway

Padova, Italy

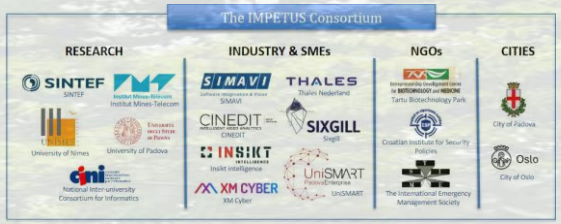
This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286.



impetus-project.eu



Thank you very much for your attention, and for filling in and sharing the IMPETUS web survey with your colleagues and friends.

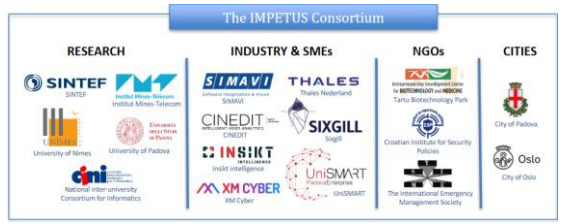


IMPETUS Public Opinion Survey on Ethical Issues on Smart Cities Technologies

Jelena Radošević
Institute for Security Policies, Croatia

IMPETUS Program on TIEMS – CBI Webinar Series
28th October at 1700 CET

Photo by Andrew Slifkin on Unsplash



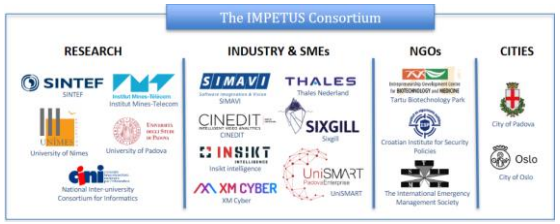
What do citizens know / want/ need / worry about?

re Smart City solutions

How?

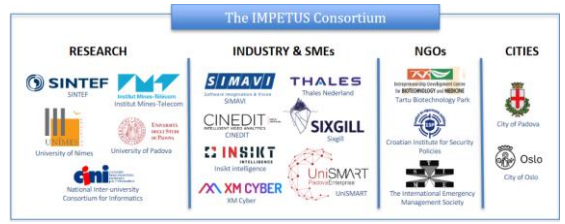
CATI

5x cca 500

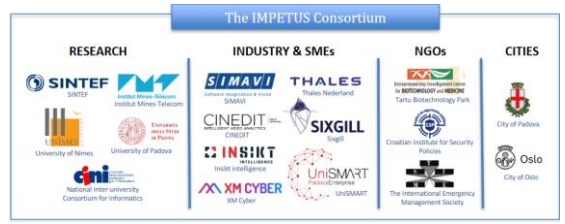


What did we actually want to determine?

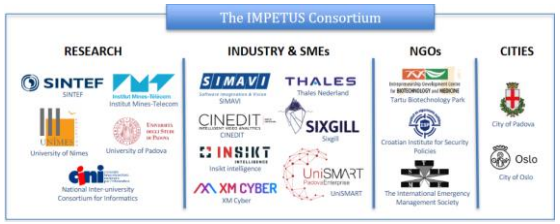
- Do citizens know what *Smart Cities* (SC) are?
- What is their opinion on SC technology in general (safety and security in public spaces included)?
- Are they thinking about / worried about the possibility of unethical use of SC technology?



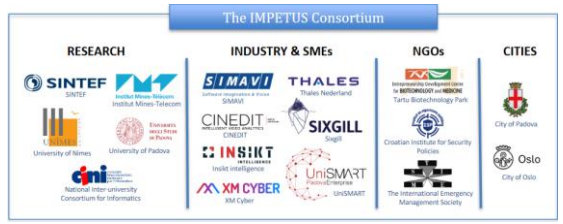
Summary	Padua	EU average	Comments
Familiarity with the concept of Smart Cities	cca 83%	cca 80%	No need for education :)
Necessity to use Smart Cities technology			
- public transportation	51%	76%	
- waste management	54%	76%	
- energy efficiency and management	47%	69%	
- smart management of healthcare	**84%**	74%	
- security	**67%**	**58%**	
- warning systems for high air pollution, danger of floods, landslides, earthquakes	**43%**	75%	
Trends in using Smart Cities technology	cca 65%	62%	*improved
Worries about the increasing level of digital skills needed for Smart Cities service	cca 8%	cca 20%	



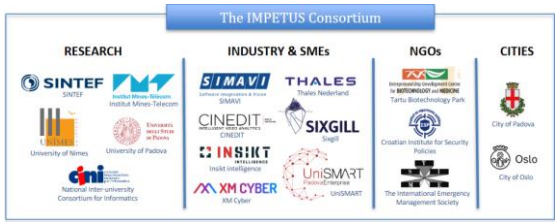
Summary	Padua	EU average	Comments
General perception of safety	cca 65%	cca 60%	
Recent change in the level of security	**46%**	18%	*improved
Violation of privacy rights and identity thefts			
- identity theft or attempted identity theft	2%	cca 10%	
- withdrawal of money from your account from an unknown source	2%	cca 10%	
- violation of privacy rights	9%	cca 20%	
- use of your personal data for unnecessary or unwanted purposes	**73%**	cca 50%	
Concern about misuse of personal information	least concerned		
Concern over the misuse of the data collected by the Smart Cities services	**7%**	42%	



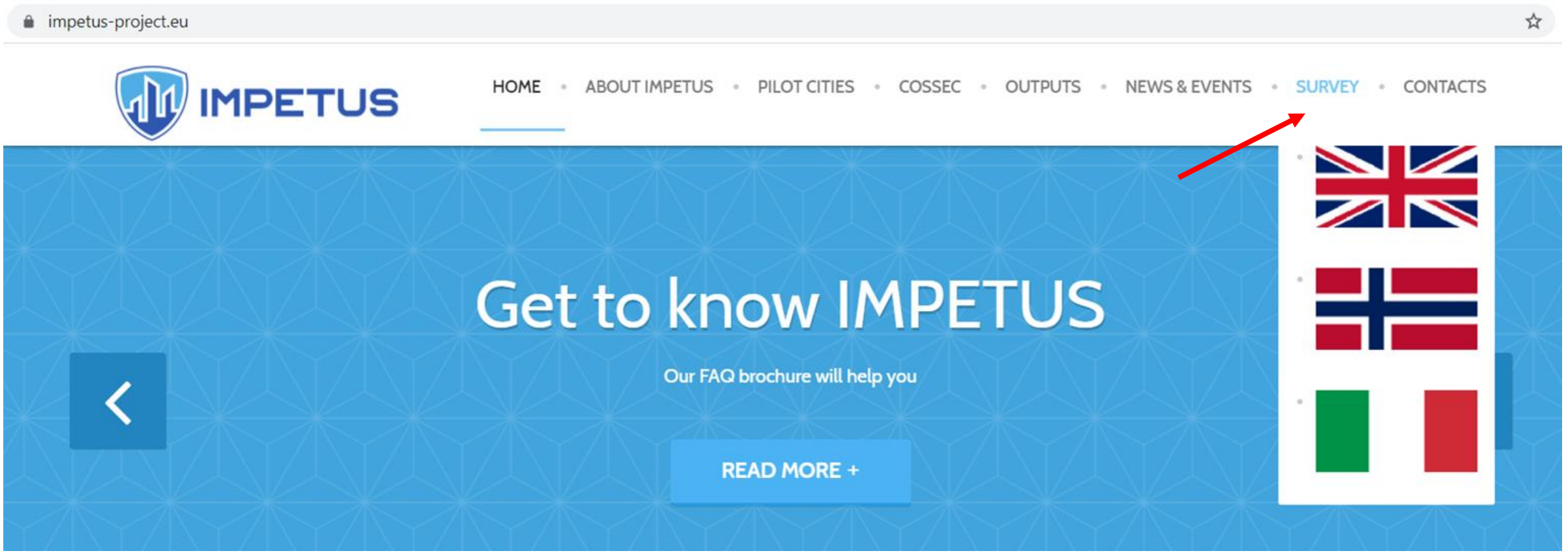
Summary	Oslo	EU average	Comments
Familiarity with the concept of Smart Cities	**cca 50%**	cca 80%	*50% never heard about it
Necessity to use Smart Cities technology			
- public transportation	**80%**	76%	
- waste management	75%	76%	
- energy efficiency and management	62%	69%	
- smart management of healthcare	64%	74%	
- security	**44%**	**58%**	
- warning systems for high air pollution, danger of floods, landslides, earthquakes	**83%**	75%	
Trends in using Smart Cities technology	cca 70%	62%	*improved
Worries about the increasing level of digital skills needed for Smart Cities service	cca 15%	cca 20%	



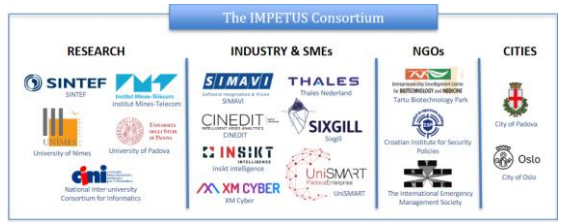
Summary	Oslo	EU average	Comments
General perception of safety	cca 80%	cca 60%	
Recent change in the level of security	71%	60%	no change
Violation of privacy rights and identity thefts			
- identity theft or attempted identity theft	15%	cca 10%	
- withdrawal of money from your account from an unknown source	17%	cca 10%	
- violation of privacy rights	21%	cca 20%	
- use of your personal data for unnecessary or unwanted purposes	44%	cca 50%	
Concern about misuse of personal information	somewhat worried		
Concern over the misuse of the data collected by the Smart Cities services	32%	42%	



impetus-project.eu



Thank you very much for your attention, and for filling in and sharing the IMPETUS web survey with your colleagues and friends.



See you in December!

For more information contact:
jelena.radosevic@insigpol.hr
Institute for Security Policies
(Croatia)
http://insigpol.hr/

IMPETUS Platform

SIMAVI
Radu.Popescu@siveco.ro

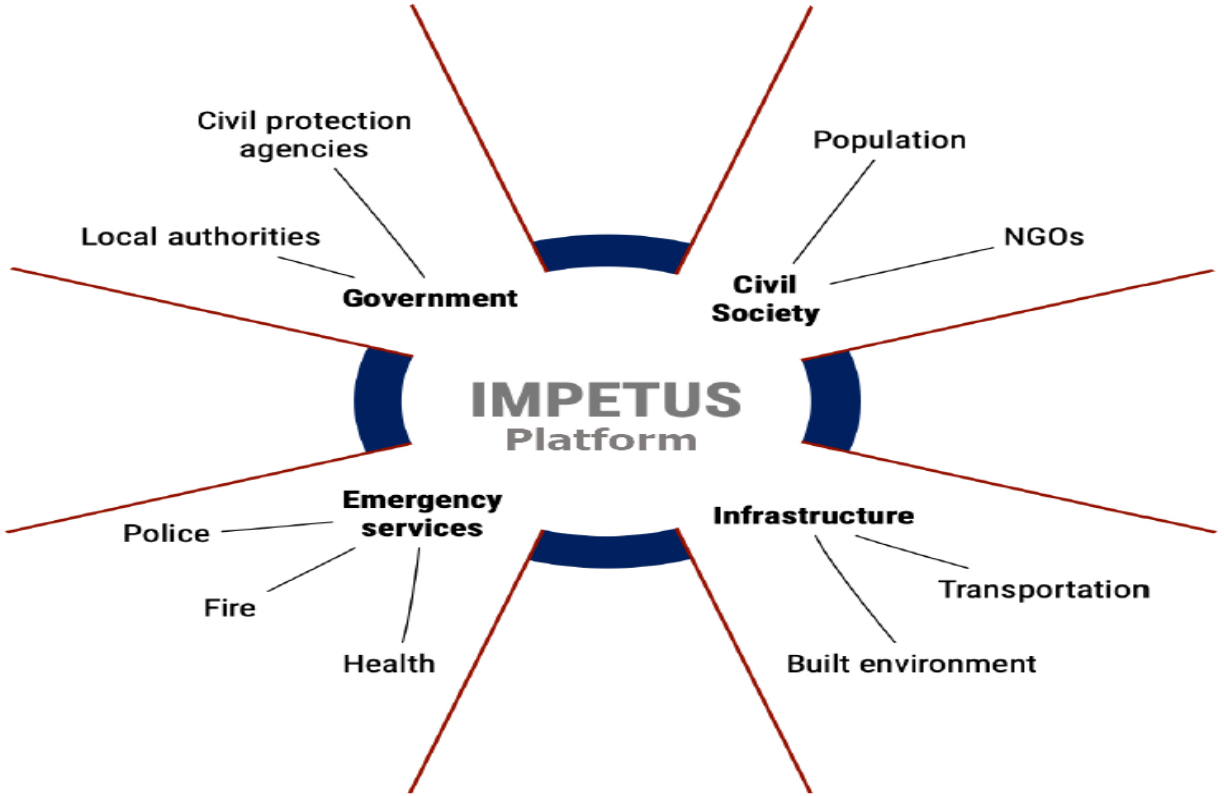
IMPETUS

Intelligent Management of Processes,
Ethics and Technology for Urban Safety

- Collecting and sharing information between security and emergency actors

- Detect threats
- Classify & monitor
- Optimize response

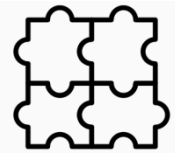
- Cla



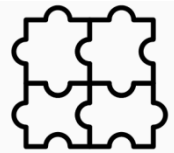
- Modular
- Interoperability
- Open & Extensible
- Future proofed
- IoT and Cloud computing approaches

Access Control

Alerting

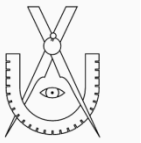


Internal Integration

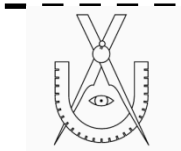


Security

External Integration



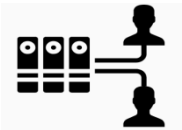
UI/UX



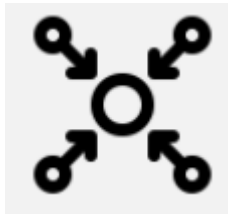
Acces rights based on roles
- Within the platform users have associated roles, which allow access to certain features

Acces control policies
- Who can access information, where and when

Simultaneous users connected
- The platform allows the connection of simultaneous users.



- Single-Sign On
- LDAP and Active Directory
- Standard Protocols
- Centralized Management of users



Alert centralisation
- The platform centralises the alerts produced by the integrated tools

Alerts displayed
- The platform displays the alerts in dashboards

Alerts priority
- The alerts have different level of attention

BRD

brd status

Location: Oslo

Timestamp: 27/10/2021 10:33:26

Bacteria level in air: 19
Water level: 1425
Bleach level: 254
Dendridiag level: 497
Standard level: 619
Drain level: 440

IMPETUS dashboard

CTI - Indicators of compromise 0s

Indicator of compromise #1632990175835

Created: 2021-03-12T09:58:36.867Z
Feed Id: darkfeed_010
Feed Name: malware_download_urls
Post Id: e064c378d37e703f124db92a206eb48a1ad75495
Post Title: x495 Netflix Premium Accounts
Source: forum_crackingportal

Indicator of compromise #1632990170834

Created: 2021-03-12T09:58:36.867Z
Feed Id: darkfeed_010
Feed Name: malware_download_urls
Post Id: e064c378d37e703f124db92a206eb48a1ad75495
Post Title: x495 Netflix Premium Accounts
Source: forum_crackingportal

Indicator of compromise #1632990165833

Created: 2021-03-12T09:58:36.867Z
Feed Id: darkfeed_010
Feed Name: malware_download_urls
Post Id: e064c378d37e703f124db92a206eb48a1ad75495
Post Title: x495 Netflix Premium Accounts
Source: forum_crackingportal

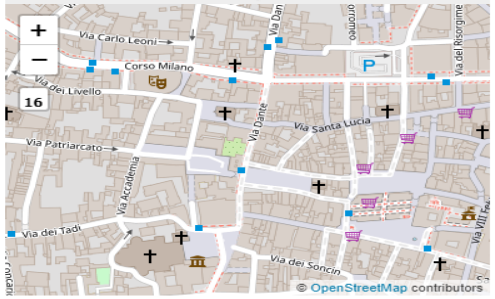
PTI 3m

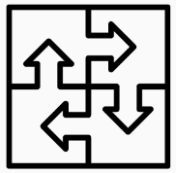
POLLEN LEVEL HIGH

MAJOR

01/01/1970 02:00:01

map



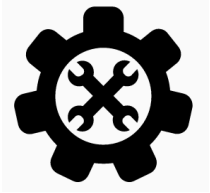


Tools integrated
- The platform is modular, individual tools can be added or removed without disturbing the functionality of the platform

Data integration
- Tool output is centralised at platform level

Data enrichment
- Outputs of the tools are combined in order to derive new information or to raise the alert confidence level

Standardised communication
- Data of the tools will respect platform defined format in order to ensure interoperability



- **IMPETUS platform should be intended to always be in operation**.
- **IMPETUS platform must be protected from outside intruders.**

- Best practices
  - Up to date software
  - User training and security awareness
  - Data protection in transit and in storage

- Vulnerability assessment

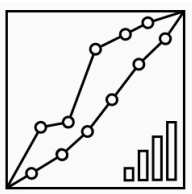
- GDPR compliance

Sharing of information
- Sharing of information to users from organisations which are not part of the IMPETUS operating environment.

Alerts for different operators
- IMPETUS platform provide alerts for different operators across different organisations.

Interaction with existing devices and platforms
- The IMPETUS platform interacts with existing devices and platforms in the cities.

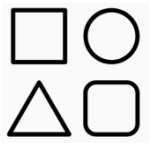
Multiple languages
- The IMPETUS platform will be available in multiple languages.

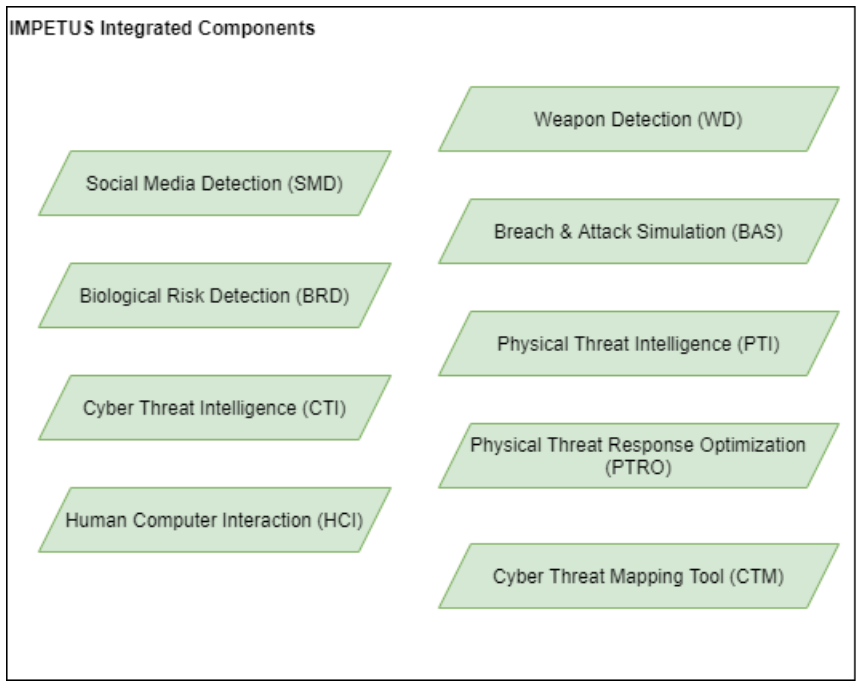


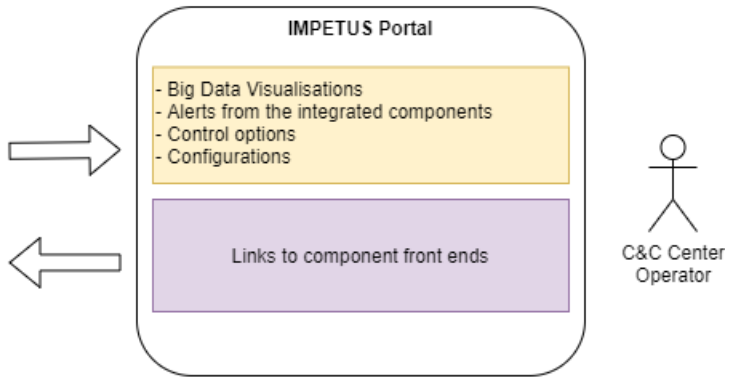
Aggregated data and diagrams
- The IMPETUS platform will provide aggregated data and diagrams to allow for strategic monitoring and planning.

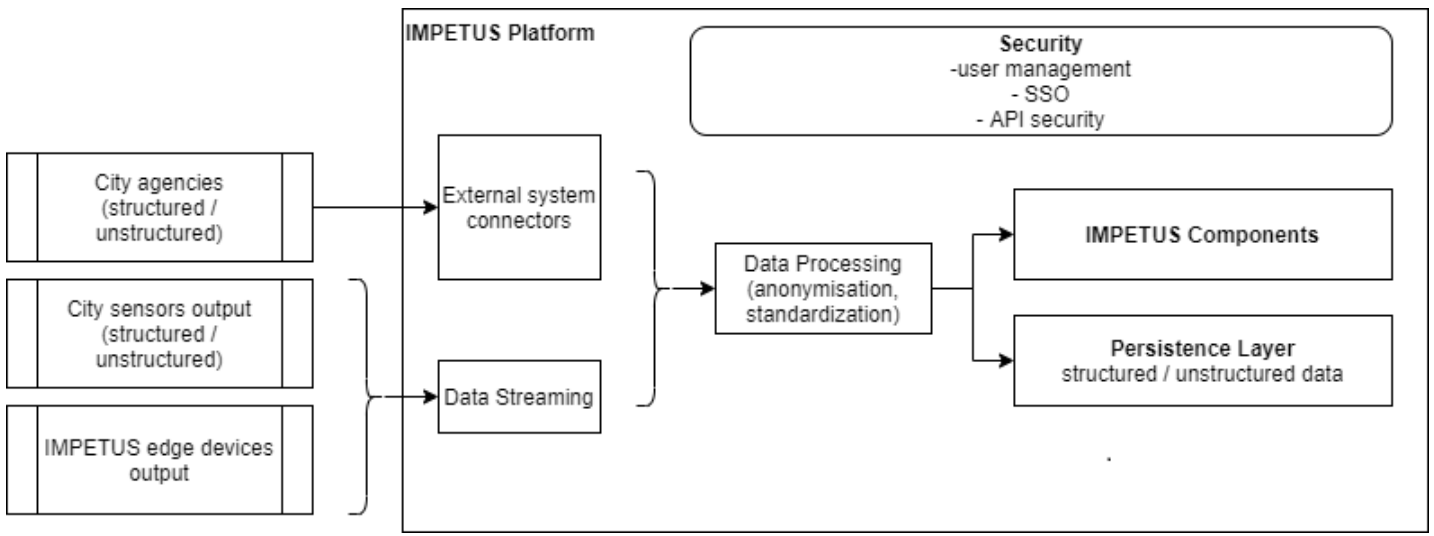
Common terminology
- The IMPETUS platform will adapt a common terminology and symbology.

Different forms of interaction
- The platform supports different forms of interaction depending on the situation and user profile



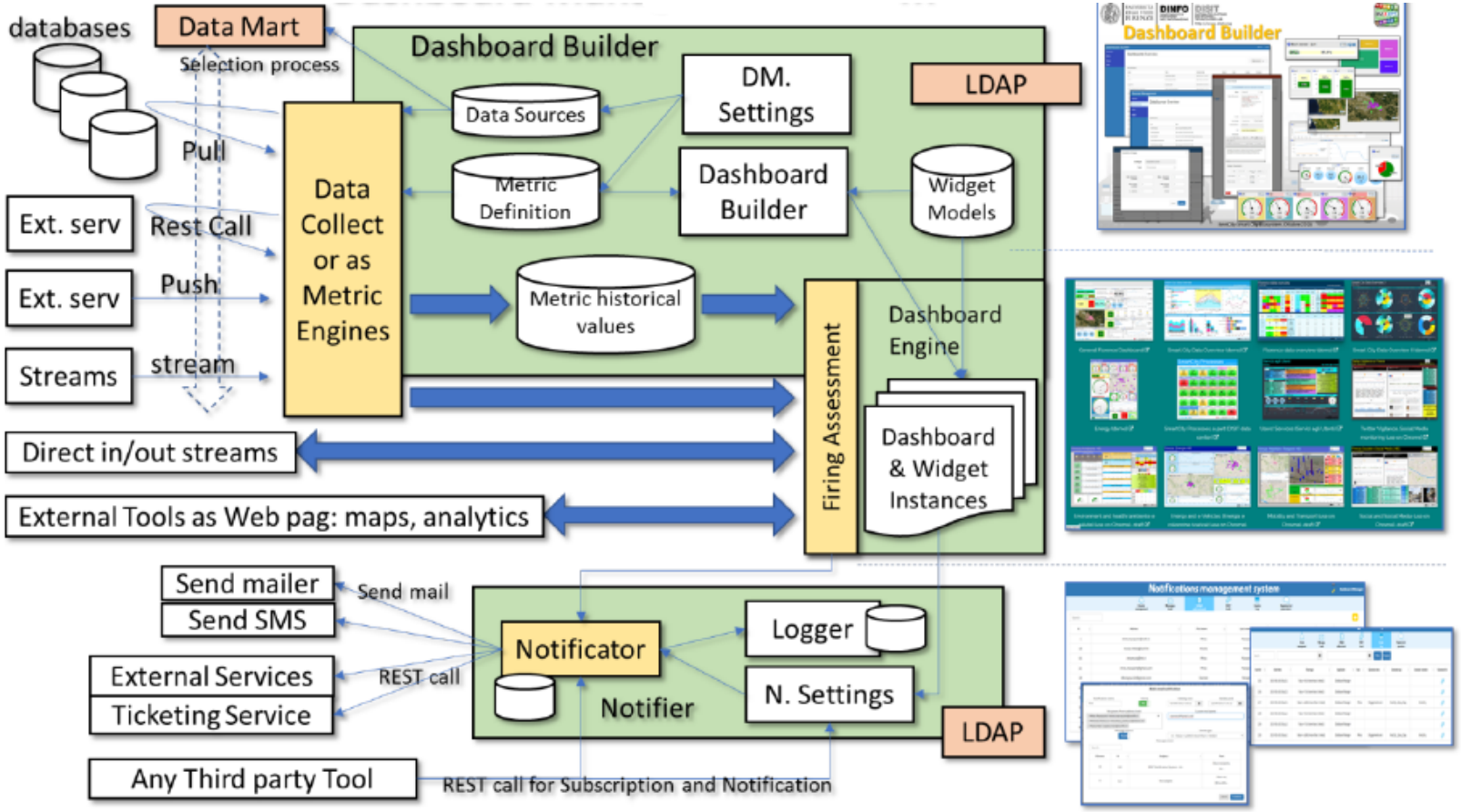

IMPETUS Integrated Components
Social Media Detection (SMD)
Biological Risk Detection (BRD)
Cyber Threat Intelligence (CTI)
Human Computer Interaction (HCI)
Weapon Detection (WD)
Breach & Attack Simulation (BAS)
Physical Threat Intelligence (PTI)
Physical Threat Response Optimization (PTRO)
Cyber Threat Mapping Tool (CTM)


IMPETUS Portal
- Big Data Visualisations
- Alerts from the integrated components
- Control options
- Configurations
Links to component front ends
C&C Center Operator

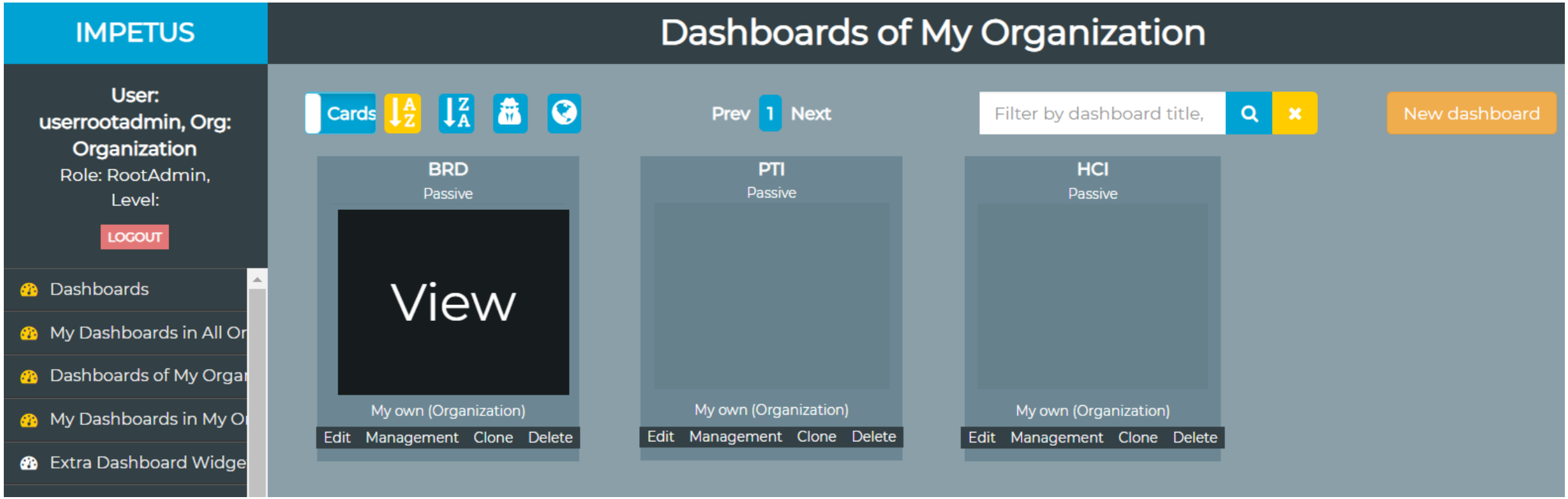

IMPETUS Platform
Security
-user management
- SSO
- API security
City agencies (structured / unstructured)
City sensors output (structured / unstructured)
IMPETUS edge devices output
External system connectors
Data Streaming
Data Processing (anonymisation, standardization)
IMPETUS Components
Persistence Layer
structured / unstructured data

Snap4City: Smart aNalytic APp builder for sentient Cities and IOT www.snap4city.org

The general architecture



Dashboard
- Every tool integrated will have an entry page in dashboard



BRD

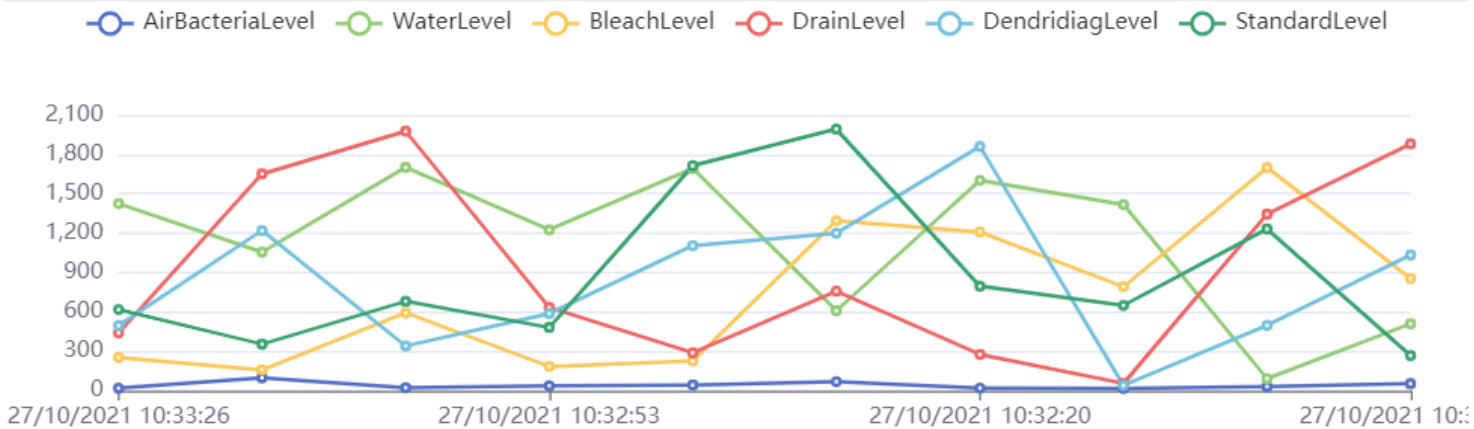
brd status 7s

Location: Oslo

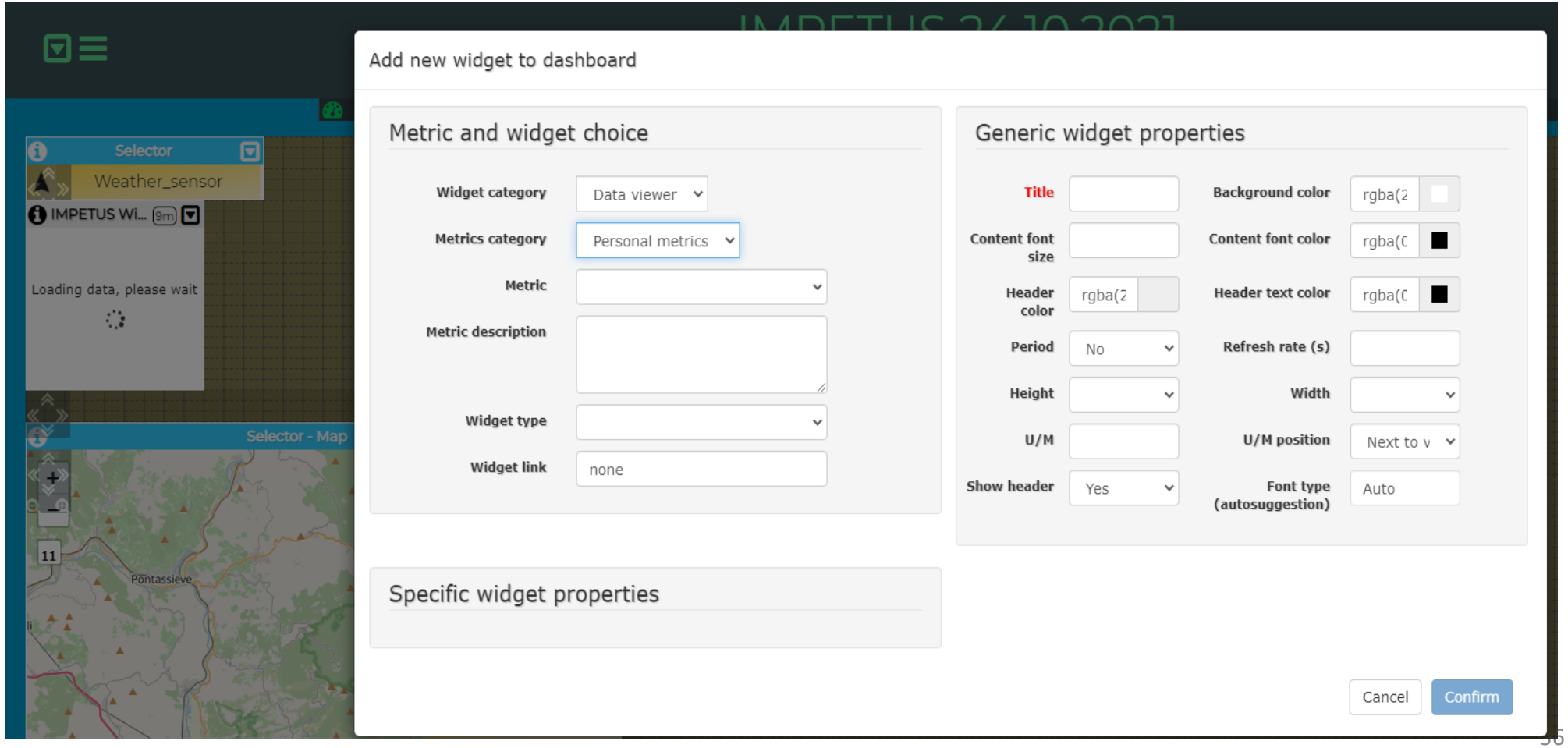
Timestamp: 27/10/2021 10:33:26

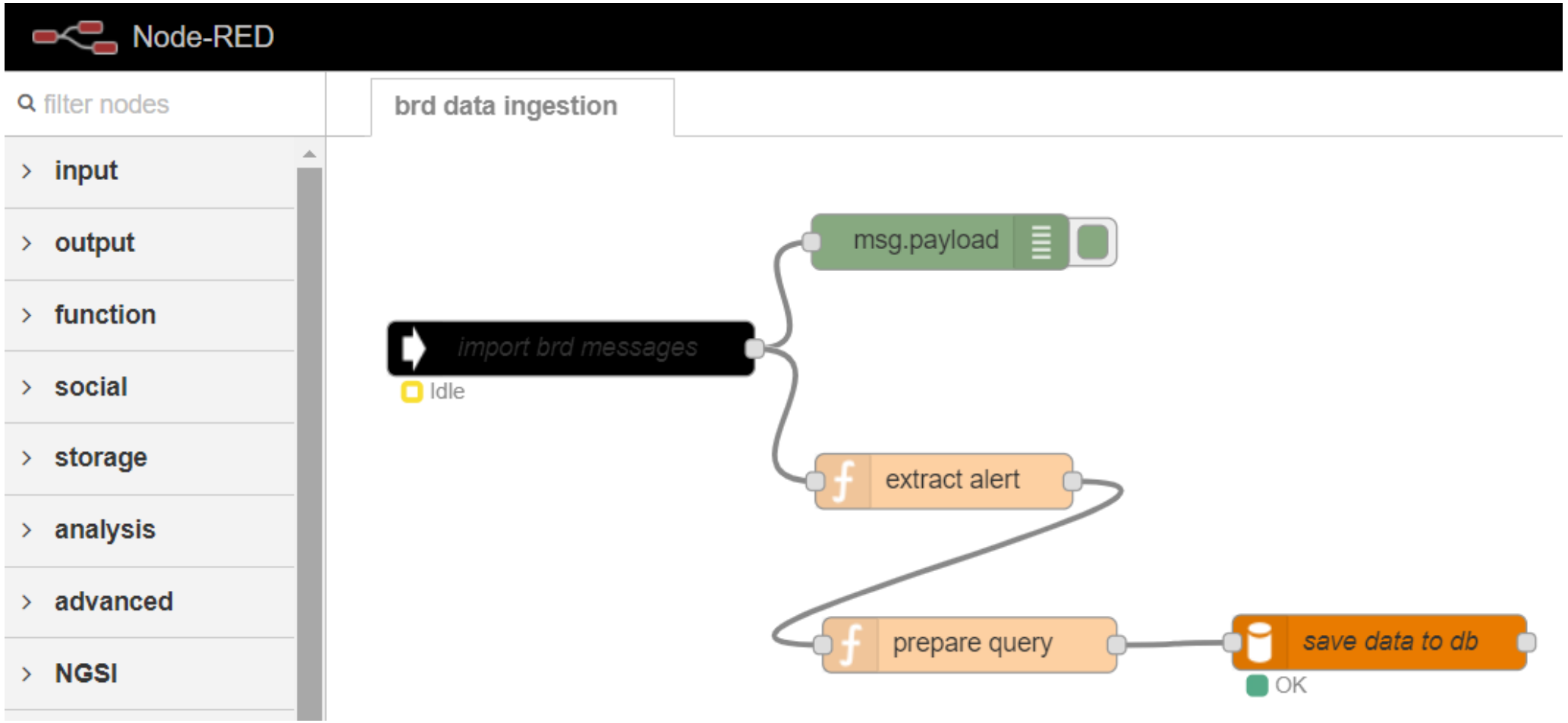
Bacteria level in air: 19
Water level: 1425
Bleach level: 254
Dendridiag level: 497
Standard level: 619
Drain level: 440

brd graphs 7s



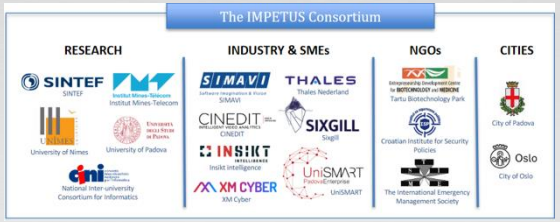
Dashboard
- Widgets can be add into Dashboard




Node-RED
filter nodes
input
output
function
social
storage
analysis
advanced
NGSI
brd data ingestion
msg.payload
import brd messages
Idle
extract alert
prepare query
save data to db
OK

Are there any questions?

IMPETUS

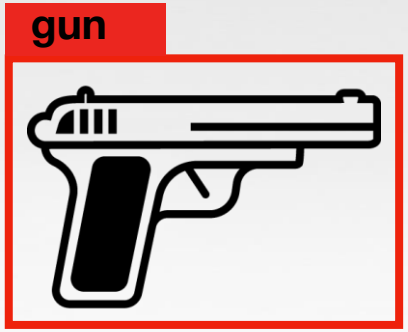


IMPETUS Weapon Detection Tool

Joachim Levy, CINEDIT, j@cinedit.com

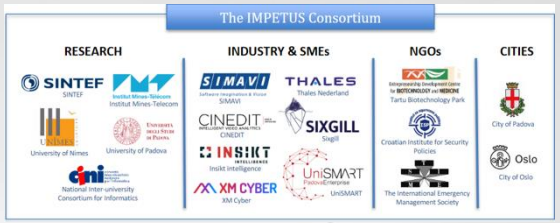
CINEDIT
INTELLIGENT VIDEO ANALYTICS

MADE IN
SWITZERLAND



IMPETUS

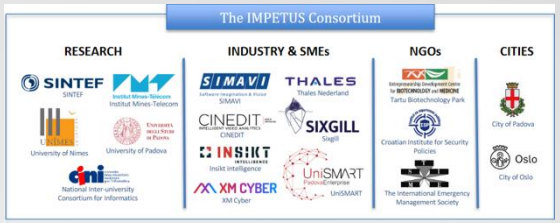
CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

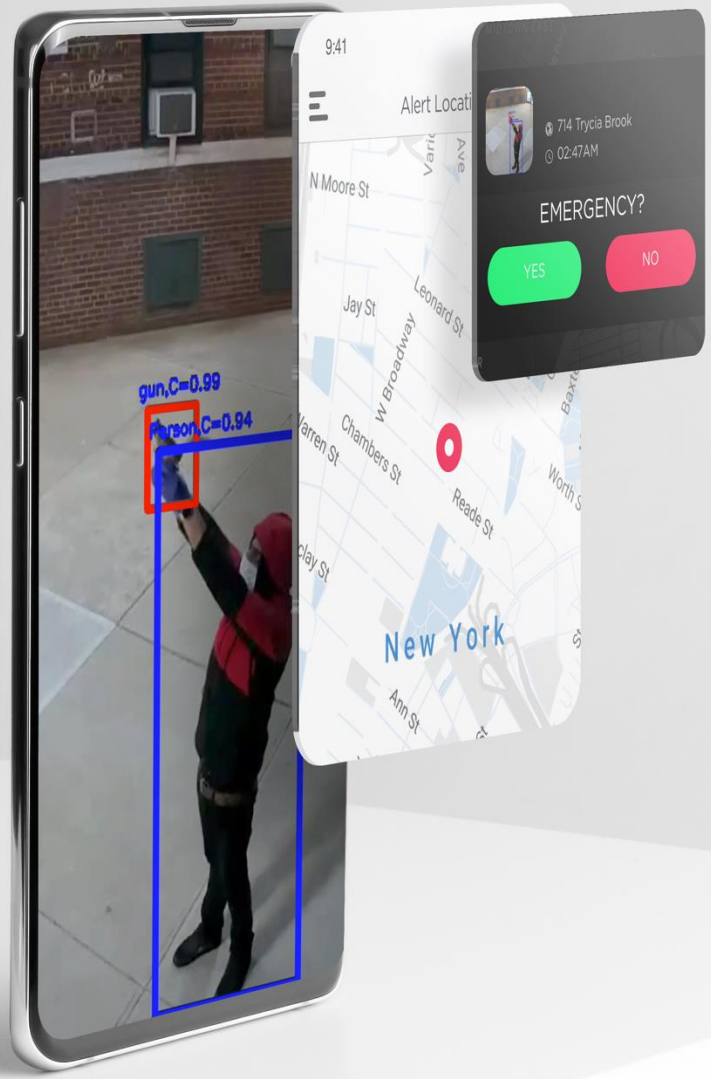


The **WEAPON DETECTION Tool's** Mission
Is To Detect Weapons To Prevent **Loss Of Life**.

IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

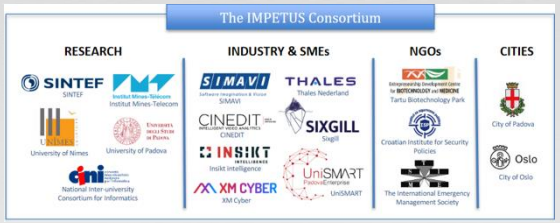




The Weapon Detection Tool
Provides Instant **SITUATIONAL AWARENESS**.

IMPETUS

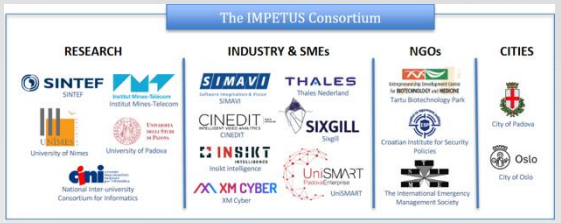
CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

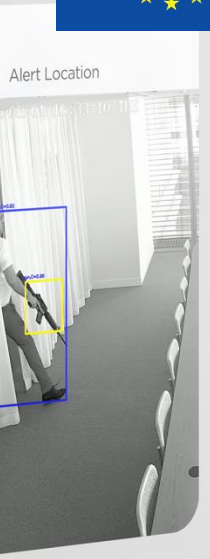


But Even When Using The Latest Machine Learning And AI Algorithms, Detecting a Weapon With Security Cameras Is **Hard**, Because The Camera Angle And The Environment Is **Never The Same**.

IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

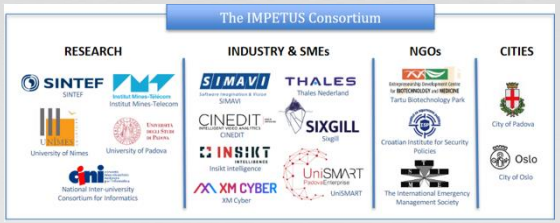




Ultimately Undetected Weapons Lead To **Expensive** Site Closure And **Loss Of Life** Because The AI They Use Cannot Be Automatically Calibrated When The Camera Angle Changes.

IMPETUS

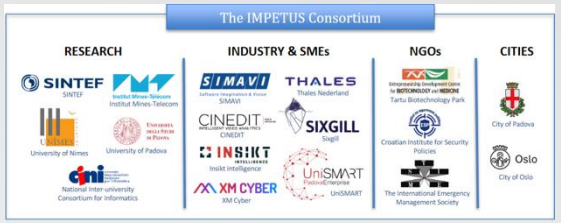
CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND



As A Result Existing Weapon Detection Systems Constantly Produce **False Alerts** And **Never** Learn From It.

IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

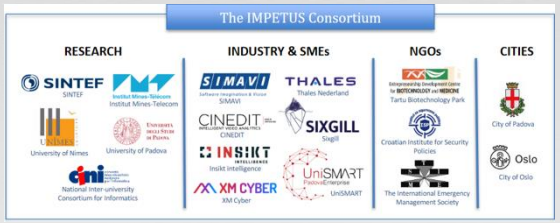


We Learn That To Detect Weapons
The AI Needs To Be **Super Accurate.**

Therefore **Data Sharing** Is **Key** To Build Better AI's.

IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

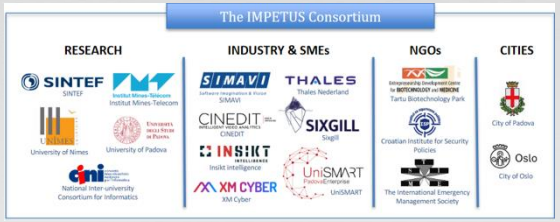


PROBLEM #1

Data Sharing Between **Smart Cities** and **High-Tech Companies** is **Very Limited** Due to GDPR Compliance.

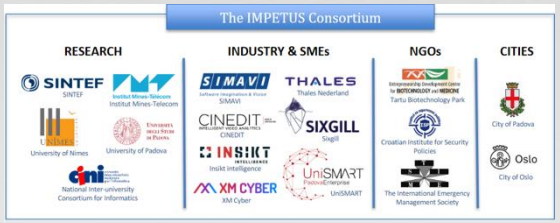
IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND



PROBLEM #2

Due To **Drifting**, The AI Keeps Becoming **Unstable** And The Predictions Keep On Becoming **Erroneous**.



PROBLEM #2

See This **Simple** Linear Regression.

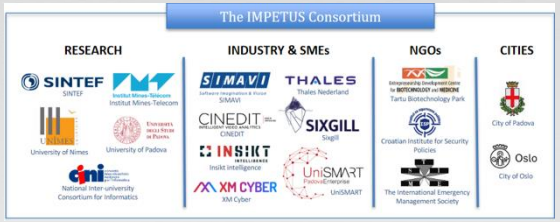
$$y = \alpha + \beta\_1*x\_1 + \beta\_2*x\_2 + \beta\_3*x\_3 + \ldots$$

We Simply Map The **Independent Variables** x_i To Predict The **Target Variable** *y* :

IMPETUS

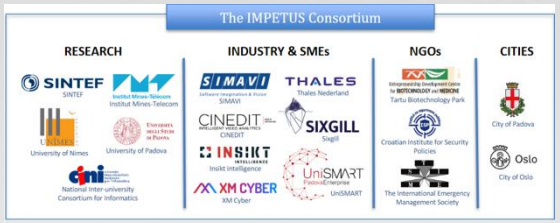
CINEDIT
INTELLIGENT VIDEO ANALYTICS

MADE IN SWITZERLAND



IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

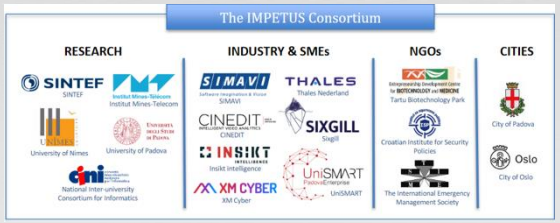


It’s Called AI Drifting

It Pretty Much Means That Any AI
Needs To Be Retrained To Remain Accurate.

IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

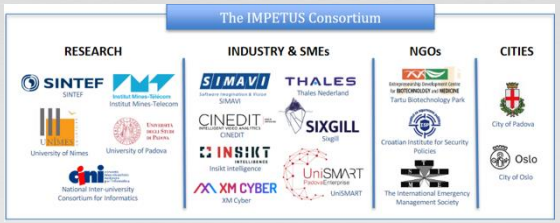


It’s An Update

Just Like When You Update An App On Your Phone

IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND



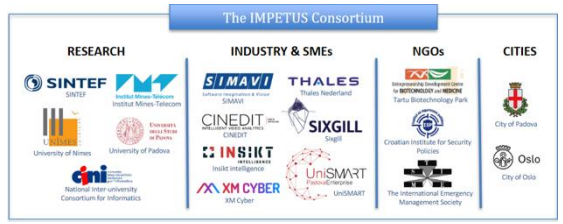
This Update Prevents Drifting

It keeps the Weapon Detection Tool **Accurate**

To do this, we need the Smart Cities to provide **Sample Data** as input to the re-training process

IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND

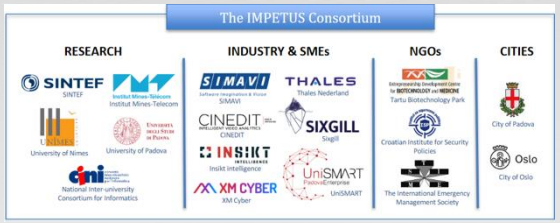


We must respect **GDPR Regulations** related to sharing of the type of sample data needed for training the AI . This can be challenging and time-consuming.

However: careful application of appropriate procedures and technical safeguards lets us share data in a GDPR-compliant way, allowing us to prevent AI drifting - and help make you **Safer.**

IMPETUS

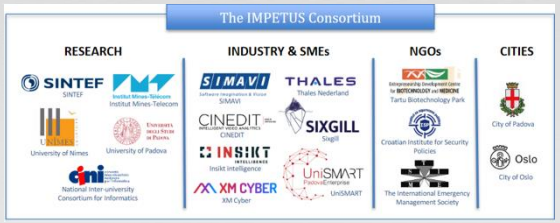
CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND



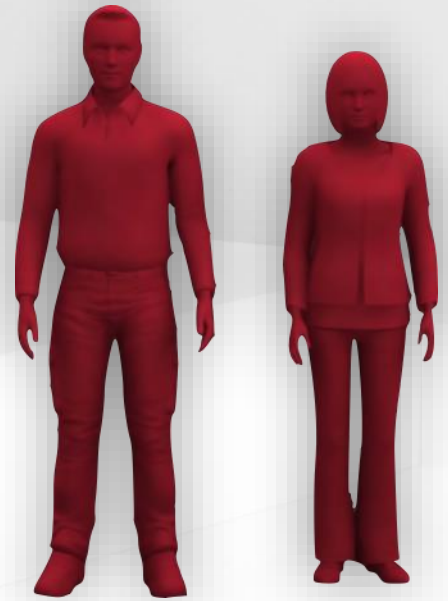
With GDPR-compliant sharing of **Sample Data**, our AI can help you remain safe and **Prevent Terror Attacks**.

IMPETUS

CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND



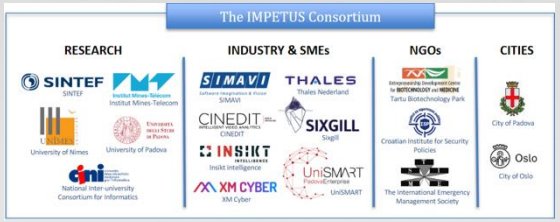
Without our trained AI, the type of event that happened at The Bataclan is more likely. **It could happen to you!**



90 Dead

IMPETUS

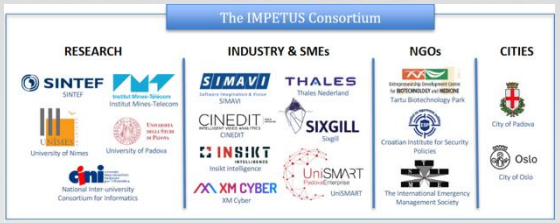
CINEDIT
INTELLIGENT VIDEO ANALYTICS
MADE IN SWITZERLAND



SO…

What Are You Going To Do **About It ?**

IMPETUS

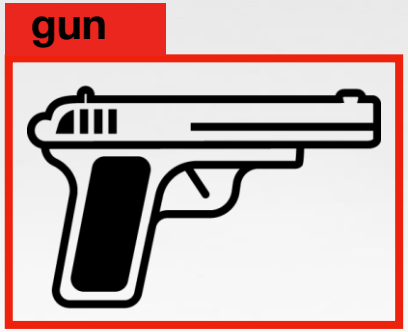


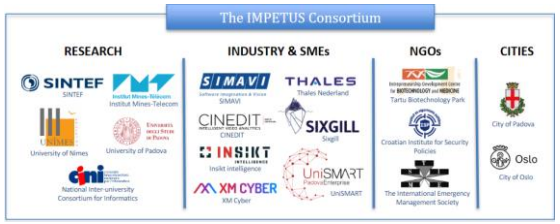
Thank you!

Joachim Levy, CINEDIT, j@cinedit.com

CINEDIT
INTELLIGENT VIDEO ANALYTICS

MADE IN SWITZERLAND

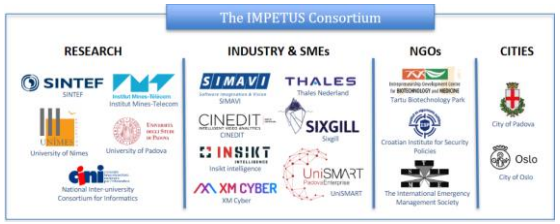




IMPETUS Social Media Detection Tool

Joaquín Luzón Tuells, INSIKT Intelligence, joaquin@insiktintelligence.com

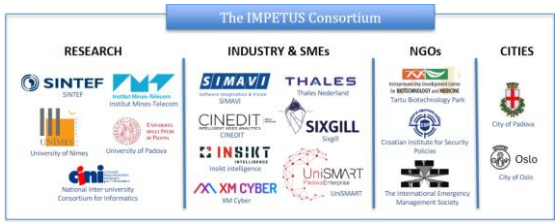
Context: INSIKT Intelligence (I)



- Social media produces too much and noisy content for the law enforcement, government and organizations alike: massive amounts of data flowing freely in a real time across multiple platforms.
  - Millions of messages per hour

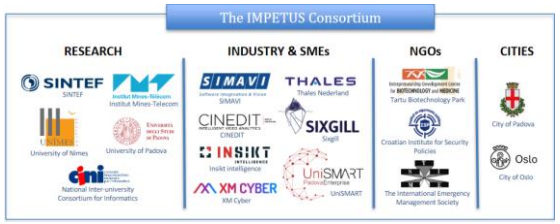
- Digital data -> Traces of criminal activity
  - Radical content
  - Terrorist messages
  - Hate speech
  - Fake news
  - Bullying
  - Harassment

Context: INSIKT Intelligence (II)



INSIKT's mission is to **harness** our technology for the **good of society** by putting **tools** with the potential to **prevent crime and save lives** in the hands of **organizations who struggle to find meaning in the data deluge produced by social media**

IMPETUS Social Media Detection tool - Technologies



Natural Language Processing

- ❑ NLP, a sophisticated Artificial Intelligence method, doesn't simply spot keywords but rather understands human written language
- ❑ Enables the processing of massive amounts of textual data without human intervention
- ❑ Facilitates the extraction of topics, concepts, entities, key ideas from any human-generated digital text data

Machine Learning

- ❑ Machine Learning algorithms create a general model based on social media data in order to interpret other data never seen before, i.e. prediction of future events, detecting sentiment or topics in social media updates without human supervision

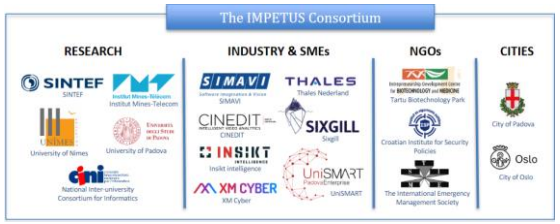
Network Analysis

- ❑ Proprietary Artificial Intelligence algorithms helping the users to understand relationships between people, organizations and events in order to piece together even the most complex puzzles

Anonymization

- ❑ Encryption of social media data to preserve privacy of individuals and comply with European and national legislations

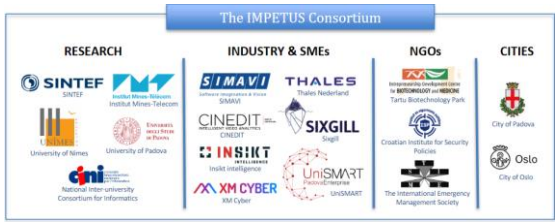
IMPETUS Social Media Detection tool



The **Social Media Detection tool**, which commercial name is **INSIKT Spotlight**, is a **unique platform**, which **collects and analyses massive amounts of online public data** to help investigative professionals **detect specific written content**, powered by **Artificial Intelligence** methods, **Data Mining**, **Text Mining** with **Natural Language Processing**, **Deep Learning**, **Big Data Analysis** and **Social Network Analysis** in order to **leverage cutting edge algorithms** to **surface hidden insights** and **cut through the noise** to. **effectively neutralise and prevent terror**, **crime and threats affecting cities**.

Insikt Spotlight: https://www.insiktintelligence.com/our-solutions/spotlight-osint/

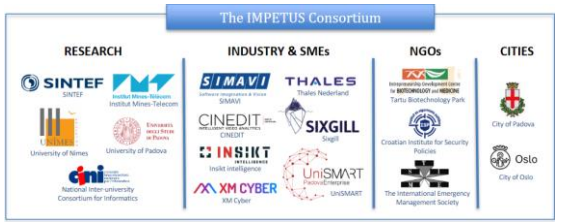
IMPETUS Social Media Detection tool – Functionalities (I)



Online data acquisition

- Data is automatically acquired, given a frequency specified for each project. The sources of data for the IMPETUS Social Media Detection tool are:
  - Twitter
  - YouTube
  - TikTok
  - Other relevant websites specific to a country or region
- By creating a project, the analyst selects which are the sources that want to include in the investigation. The tool integrates scrapers adapted to each source. All the acquired data is shown in the dashboard as raw anonymised data and also within the different analysis.

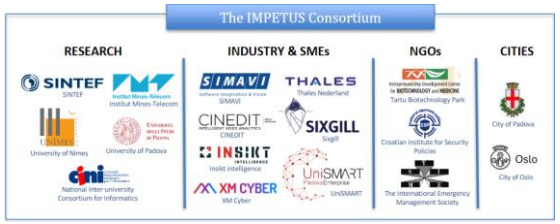
IMPETUS Social Media Detection tool – Functionalities (II)



Linguistic feature identification

- Seven different methodologies of Natural Language Processing are applied in 5 languages: English, Italian, Norwegian, French and Arabic.
- The analysis of the text is made from different perspectives:
  - Concepts extraction
  - Key Ideas extraction
  - Topic classification
  - Hate Speech detection
  - Entities extraction
  - Hashtag detection
  - Sentiment analysis

IMPETUS Social Media Detection tool – Functionalities (III)



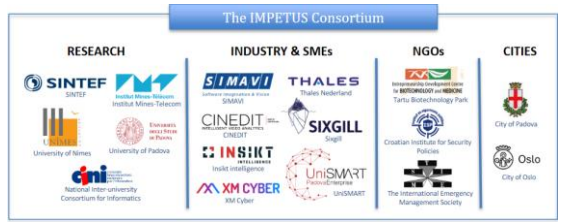
Social Network Analysis

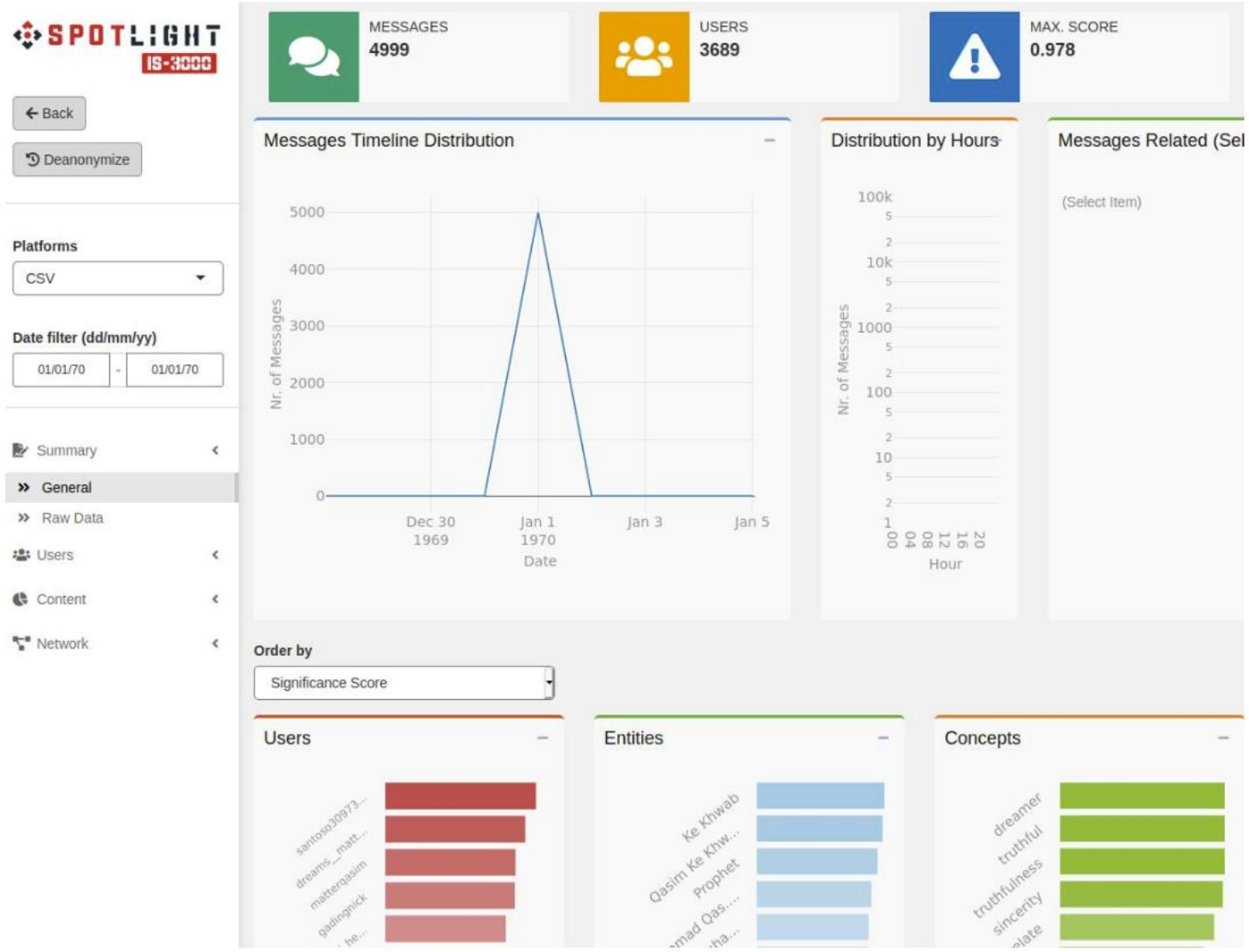
- Analysis of observed interactions creating relationships relations between authors within Social Media.
- This analysis gives information about the users in terms of their activity within the Social Media, and their score as influencers, spreaders, and the role they have.
- Communities within Social Media are also detected and analysed.

Hate Speech

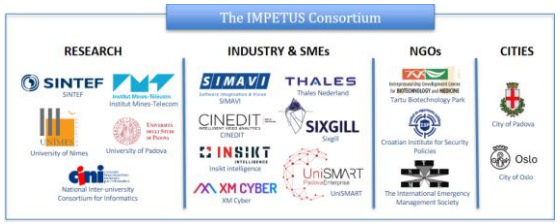
- The text extracted from the social media and the local newspapers are analysed to evaluate the degree of hate speech they have.

IMPETUS Social Media Detection





IMPETUS

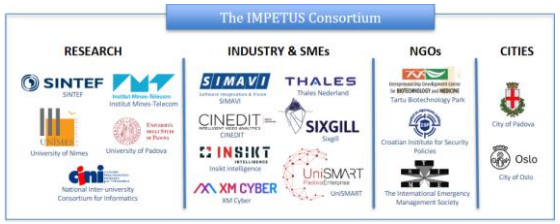


Thank you!

Joaquín Luzón Tuells, INSIKT Intelligence, joaquin@insiktintelligence.com

INSIKT INTELLIGENCE

OSLO



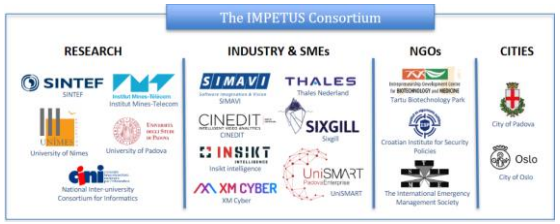
IMPETUS Solutions
Implementation in City of Oslo

Osman Ibrahim
Agency for Emergency planning
City of Oslo, *Norway*

Oslo

IMPETUS Program on TIEMS – CBI Webinar Series
28th October at 1700 CET

OSLO

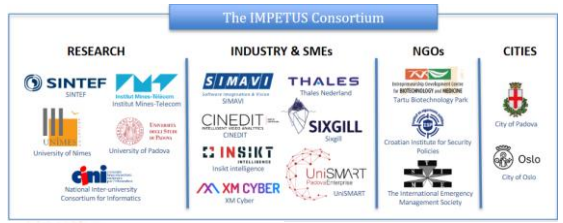


- Oslo is the capital of Norway and the country's largest city with over 650,000 inhabitants.
- Compact capital city surrounded by the Oslo Fjord on its south side and the forest areas east, north and west
- Very accessible city and Norway's hub for national and international travel
- Hostcity for large events/international events

The City of Oslo holds both municipal and county functions

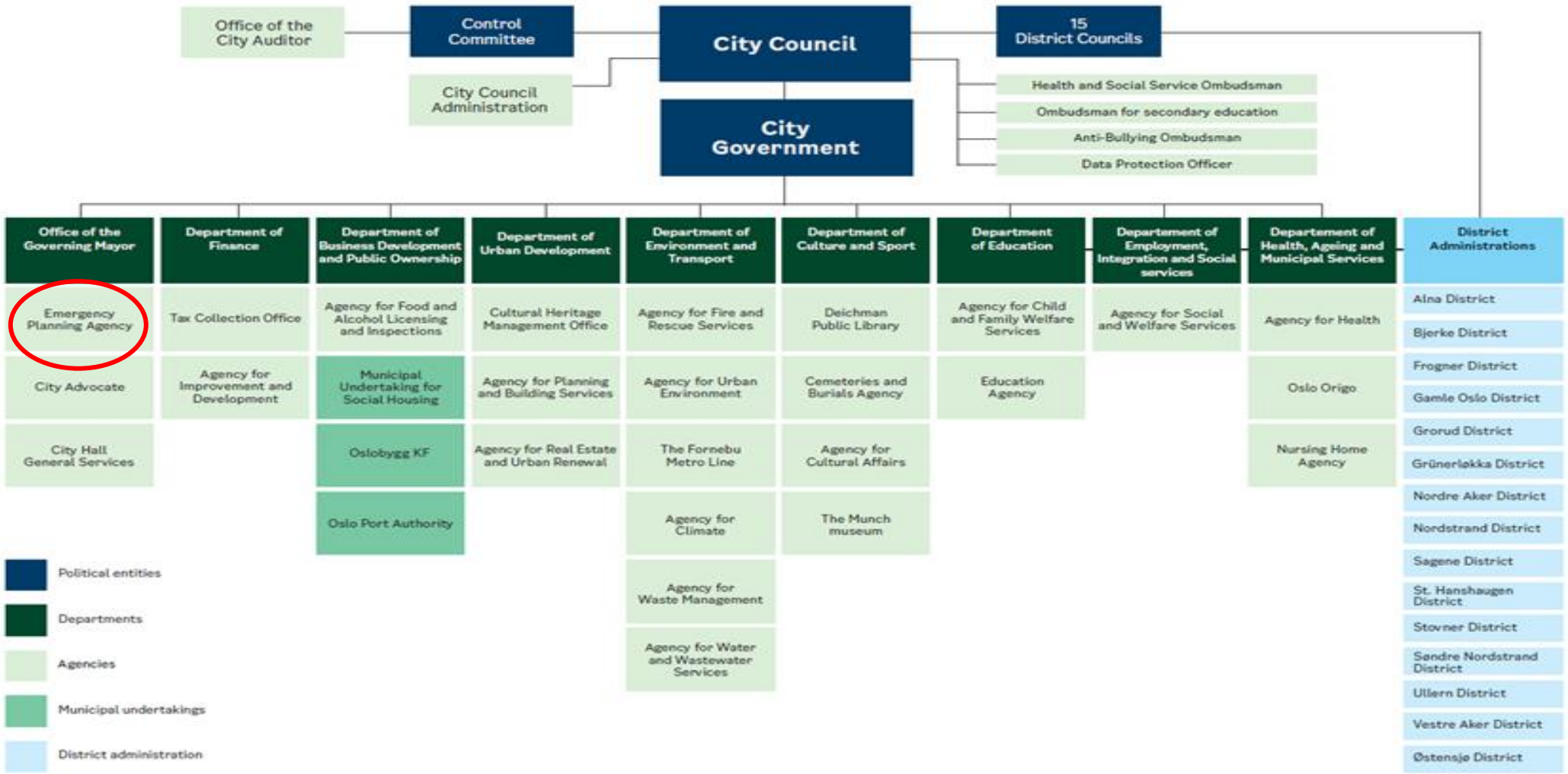
- Oslo Central Station bombing in 1982
- The Norway attacks 22th july 2011

OSLO

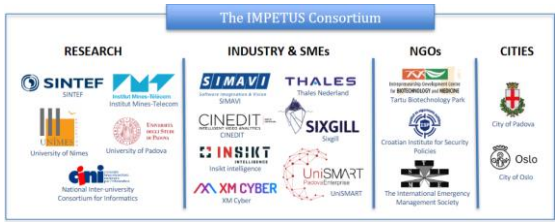


Oslo

Organizational chart City of Oslo



OSLO

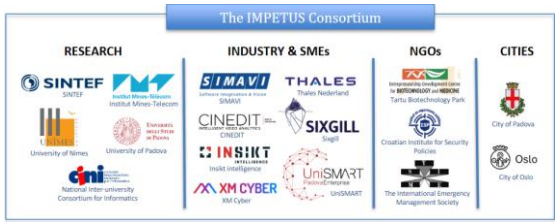


- Covid pandemic addressed new needs for insights in public opinions and understanding effects of implemented measures

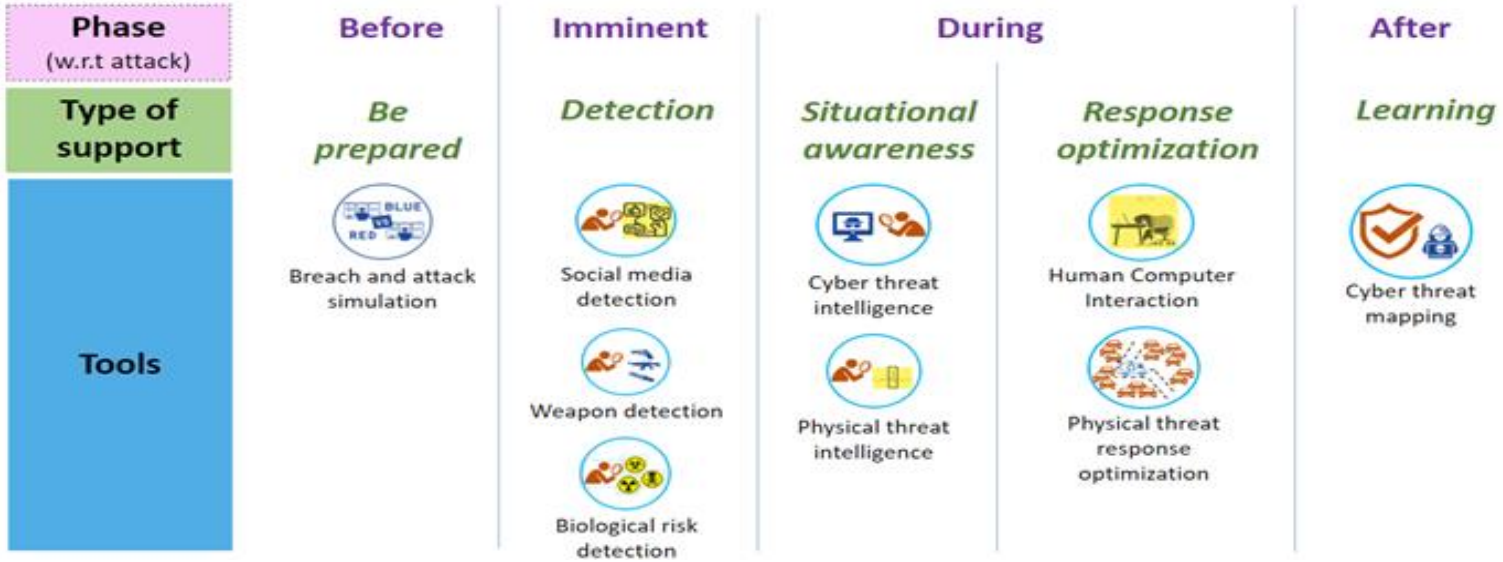
- We have broken an important barrier under Covid
  - Actively using information about and from citizens in our intelligence and risk communication
  - New sources such as mobility data, healt data etc.

- We as individuals are the risk of spreading the virus
  - Closer on focusing on risk exposure at individual level
  - Covid risk vs threats ?

OSLO

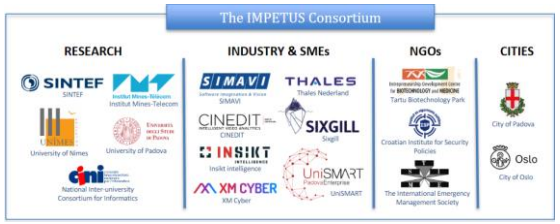


- Increase level of early detection and ability to provide indicators for predictive analysis and response
  - security and safety incidents
- Simplifies manual processes with greater data acquisition
- Optimization of knowledgebased response



- Promotes increased and cross-sectorial common situational awareness
- Implementation of IMPETUS in a wider environment that works, holistically, systematically, and cross-sectorially with all risks we are exposed to

OSLO



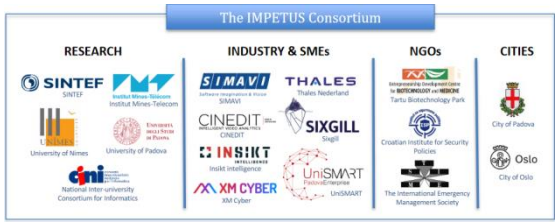
Smart City Center – Risk operations Centers (ROC)

The SOC process:

1. Expanding insight/information collection
2. Expanding analysis capacity and areas
3. Response activation
4. Evaluation and correction of response

UN sustainable development goals Target 11b: *Implement Policies for Inclusion, Resource Efficiency and Disaster Risk Reduction. Resilience.*

✓ We expect to expand the applications of IMPETUS technologies



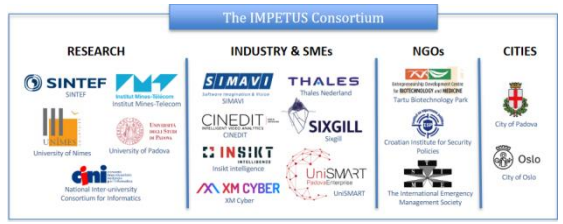
IMPETUS – COSSEC Network

Sandro Bologna – TIEMS Belgium

CBI Webinar

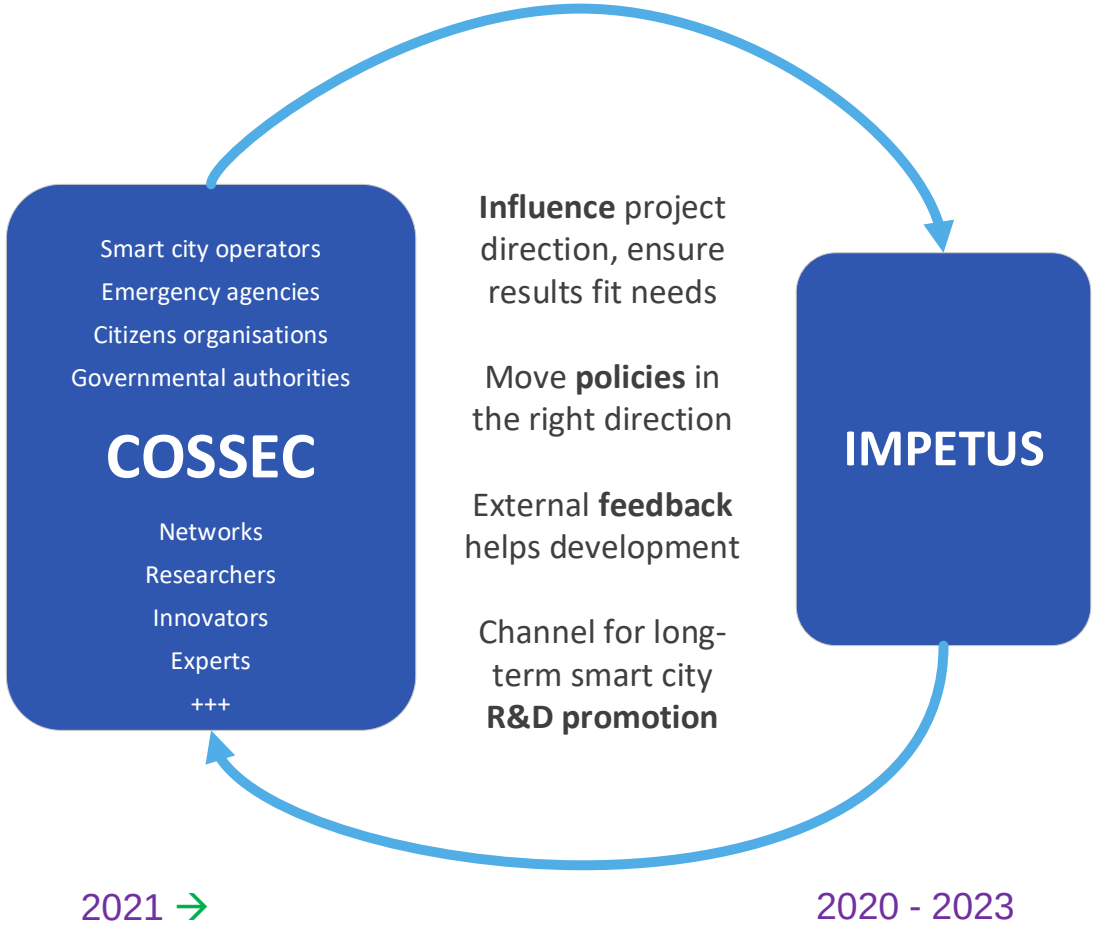
28th October 2021, 17:00 CET

What is COSSEC

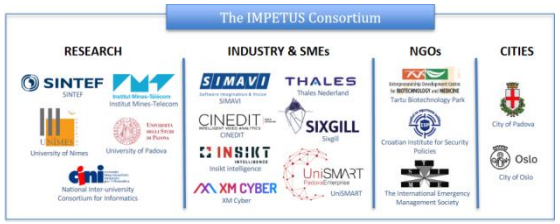


COSSEC stands for **"Community of Safe and Secure Cities"**. It is a group of individuals representing organisations or projects that have an interest in or might be affected by the work being done by the IMPETUS project. The first steps in establishing the community were made even before the project started, and one of the tasks in the project is to develop and foster COSSEC. We foresee that COSSEC will continue after the end of the IMPETUS project itself, as a forum for organizations interested in using IMPETUS results, or with a wider interest in the topics addressed by the project.

The idea of COSSEC is to extend involvement in the project to stakeholders beyond the project consortium. COSSEC members will **influence IMPETUS activities** so that solutions emerging from the project will meet local needs in other cities and/or meet other concerns or requirements they might have. Some COSSEC members will be early adopters of project results.



COSSEC Status at 22.10.2021



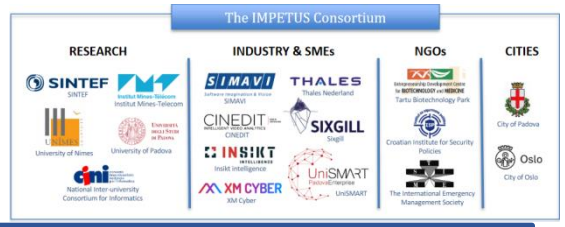
COSSEC expectation from IMPETUS DoA (Description of Activities)

Number of members: > 40 members
Diversity of members: > 10 cities
Diversity of members: > 5 citizen groups
Diversity of members: > 10 EU countries
Number of Workshops: = 2
Number of Webinars: = 2

COSSEC Status
October 22, 2021

Number of members: 24 (for details see COSSEC Platform https://pr4gdm.giftmaru.com/)
Diversity of members: 6 cities (for details see COSSEC Platform https://pr4gdm.giftmaru.com/)
Diversity of members: 1 citizen group (for details see COSSEC Platform https://pr4gdm.giftmaru.com/)
Diversity of members: 11 EU countries (for details see COSSEC Platform https://pr4gdm.giftmaru.com/)
Number of Workshops: 0 (limited by COVID-19)
Number of Webinars: 2 (for details see COSSEC Platform https://pr4gdm.giftmaru.com/)

1st COSSEC Webinar
04.05.2021



USE OF ADVANCED IT FOR THE PROTECTION OF PUBLIC SPACES
Virtual Meeting, May 04, 2021, 4 p.m. to 6 p.m. CET

4 p.m Presentations of Projects and Initiatives (chaired by COSSEC Sandro Bologna)

IMPETUS - Intelligent Management of Processes, Ethics and Technology for Urban Safety (H2020)
Joe Gorman (SINTEF), Matthieu Branlat (SINTEF)

SURE - Smart Urban Security and Event Resilience (UIA Initiative)
Autero Anniina (Tampere), Säpyskä Minna (Tampere)

Snap4City - Firenze Smart City Control Room (International)
Paolo Nesi (University of Florence)

Open & Agile Smart Cities (OASC International)
Davor Meersman, Ricardo Pinho, Gert De Tant (OASC International)

5 p.m. Plenary discussion around the most challenging topics (chaired by IMPETUS Matthieu Branlat)

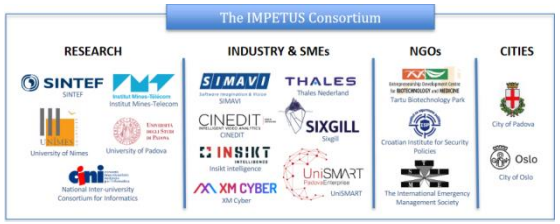
Security technology application for the protection of public spaces
with contributions from IMPETUS: Joaquin Luzon (Insiktintelligence) and Joe Levy (Cinedit)

Operational impact of security technology application for the protection of public spaces
with contributions from IMPETUS: Lars Ole Grottenberg (OSLO Kommune)

6 p.m. End of the virtual meeting

To get copies of the presentations go to https://pr4gdm.giftmaru.com/
Section: Activities/Events/Virtual Meeting May 4th, 2021

2nd COSSEC Webinar at 16.06.2021



Ethical and Legal Issues with the use of Smart Cities Technologies for Public Protection
Virtual Meeting, June 16, 2021, 2 p.m. to 4 p.m. CET

2 p.m Introduction to the Virtual Meeting Sandro Bologna (COSSEC Chair)

Survey on use of Smart Technologies in Detecting Security Threats in Public Spaces - Ethical Issues (ISP IMPETUS Partner - Croatia)

Ethical Issues, personal data protection and possible misuses of personal data: a European perspective
(COSSEC Member Luigi Carrozzi - Expert of personal data protection - Italy)

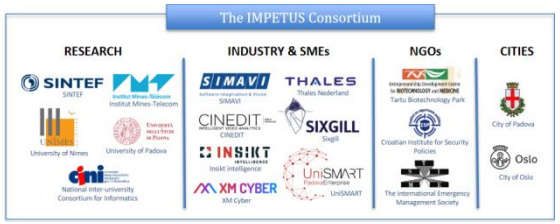
Ethical Issues of perceived fairness in Machine Learning (ML) (COSSEC Member Deepak Khazanchi -University of Nebraska at Omaha, USA)

Open Discussion about some controversial claims (Chaired by Krunoslav Katic – ISP IMPETUS Partner)

4 p.m. End of the virtual meeting

To get copies of the presentations go to https://pr4gdm.giftmaru.com/
Section: Activities/Events/Virtual Meeting June 16th, 2021

Invitation to join COSSEC



Projects and initiatives to improve the security of public spaces and community resilience are invited to apply for joining COSSEC

If you want to learn more about COSSEC, please contact:

Sandro Bologna, TIEMS, s.bologna@infrastrutturecritiche.it

or visit

the dedicated COSSEC Platform at https://pr4gdm.giftmaru.com/