APPRAISE

Facilitating public & private security operators to mitigate terrorism scenarios against soft targets

D10.4 – MARKET ANALYSIS

Lead beneficiary	CS
Type of document	Report
Dissemination Level	[PUBLIC]
Due date	30/11/2022
Submission date	26/01/2022
Main Author(s)	Yana Lazarova (CS)
Contributors	All technical partners

This project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 101021981

PROJECT INFORMATION

Grant Agreement Number	101021981
Acronym	APPRAISE
Name	Facilitating public & private security operators to mitigate terrorism scenarios against soft targets
Topic	SU-FCT03-2018-2019-2020: Information and data stream management to fight against (cyber)crime and terrorism
Funding Scheme	Innovation action
Start Date	01/09/2021
Duration	30 Months
Coordinator	CS GROUP - FRANCE

REVISION HISTORY

Version	Date	Author	Comments
V0.1	06/10/2022	Yana Lazarova (CS)	ToC and a first draft of executive summary paragraphs
V0.2	07/10/2022	Yana Lazarova (CS)	Sent to technical inputs to partners
V0.3	10/01/2023	Yana Lazarova (CS)	Last partner contribution integrated
V0.4	13/01/2023	Alexandre Ahmad (CS)	Internal Review
V0.5	19/01/2023	Damian Puchalski (ITTI)	Quality review by ITTI
V0.6	23/01/2023	Leonardo Napoletani (ATK)	Quality Review by ATK
V1.0	26/01/2023	Yana Lazarova (CS)	Quality Review comments integrated Final version.

QUALITY REVIEWERS

Name	Organisation
Damian Puchalski	ITTI
Leonardo Napoletani	ATK

SECURITY REVIEW

Name	Organisation	Status
Denis Caletta	ICSS	[Passed]

EXECUTIVE SUMMARY

The present document describes the market analysis for the APPRAISE platform as a whole, as well as the market analysis for each individual tool of the APPRAISE framework. At this stage of the project the Market analysis identifies the market situation, trends, size and segmentation, along with the competitors, partners and provides. This analysis is complemented by a SWOT analysis. This enables partners to have a clear preliminary vision of the marketability of the APPRAISE platform and of their own product, thus preparing the commercialisation of the products.

Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 101021981.

ABBREVIATIONS

AI	Artificial Intelligence
AR	Augmented Reality
ATM	Automated Teller Machine
C/P	Cyber and Physical
C-UAS	Counter UAV System
C2	Command and Control
CAGR	Compound Annual Growth Rate
CBRN	Chemical, Biological, Radiological, Nuclear
CCTV	Closed-Circuit Television
CERN	European Organisation for Nuclear Research
CPNI	Centre for the Protection of National Infrastructure
DITHO	Digital Twin-based Hypervision and Operation Management System
EC	European Commission
ENISA	European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
GIS	Geographic Information System
GPS	General Positioning System
HTML	HyperText Markup Language
ICT	Information and Communication Technologies
IPR	Intellectual Property Rights
ISAR	Interactive Streaming for Augmented Reality
ISO	International Organisation for Standardization
LCMR	Lightweight Counter Mortar Radar
LEA	Law Enforcement Agency
MoD	Ministry of Defence
OSINT	Open-source Intelligence
OT	Operations Technology
POS	Point of Sale

PPI	Producer Price Index
SELP	Social, Ethical, Legal and Privacy
SWOT	Strengths, Weaknesses, Opportunities, Threats
TRL	Technology readiness Level
UI	User Interface
VIP	Very Important Person

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF THE DOCUMENT

This document aims at creating a solid base for the exploitation of the APPRAISE platform. Its objective is two-fold, on one hand it analyses the potential market for the APPRAISE platform, combining the multiple tools developed within the project. On the other hand, it analyses the potential market for every technological brick of the platform.

The purpose of D10.4 "Market analysis" it to clearly identify potential markets for each tool. Despite the fact that some tools are still under development in research centres, a clear market and utility has been identified. Furthermore, drivers and barriers are also presented for each tool. This approach enables APPRAISE partners and the project as a whole to envisage different market strategies targeting specific and existing markets, that have been studies and analysed in advance.

This deliverable is the outcome of Task 10.3 that has for objective to prepare and keep updated a market analysis performed by each result owner. The analysis has been performed for each component and on the overall APPRAISE platform. Due to the public nature of the document confidential information has not been included.

Throughout the project the market trends and possibly evolving needs will be closely followed in order to better adapt the exploitation strategy for the APPRAISE platform and each module. This continuous analysis will be used in upcoming deliverable focusing on exploitation and market uptake.

This document is closely linked to:

Del. N°	Deliverable title	Lead beneficiary	Due date
D10.5	Exploitation strategy and Business model	ENG	M18
D10.6	Final exploitation, IPR and market uptake plans	ENG	M30

1.2 INTENDED AUDIENCE

This deliverable is public, and its intended audience includes:

- APPRAISE Project Partners: as a reference for the current market status and the possibilities to commercialize the APPRAISE platform and individual technological solutions.
- European Commission: visibility on the added value of the APPRAISE technologies and the contribution of the project towards the safety and security improvement in public spaces.
- General public: visibility on innovative technologies developed within European Projects.

1.3 STRUCTURE OF THE DOCUMENT

This document is structured in 6 Sections:

Section 1: Introduction presenting the purpose, the intended audience and the structure of the document.

Section 2: Identifying the different components of the APPRAISE platform.

Section 3: Market analysis of the APPRAISE platform as whole.

Section 4: Market analysis of the APPRAISE components. This chapter is broken down per types of tools to be developed.

Section 5 provides the conclusions, while Section 5 summarises the references.

2 IDENTIFICATION OF COMPONENTS

APPRAISE aims at developing and validating a state-of-the-art framework for soft target protection. The focus of the project is on the active, audited and well-defined information and intelligence exchange between public and private security actors in order to enable efficient collaboration, at both information and operational levels. The above-mentioned framework is composed by a set of tools that can each, separately or combined together, enhance the operational capacity of LEAs, private security operators, and especially their collaboration to improve the operational capacity to protect soft targets from attacks. The APPRAISE tools can be divided in five major categories, where each will develop a set of innovative technologies.

The table below summarises the different components per technological category and field of use, namely:

- Novel tools for real-time early detection of security threats in public spaces
- Actionable intelligence for proactive security
- Internet content analysis tools
- Public-Private interoperability and collaboration services
- Visualization and DSS services

A market analysis focusing on the market situation, trends, size and segmentation has been conducted, along with the identification of competitors, partners and providers. The analysis of each tool is complemented by a SWOT analysis.

The following three tools developed by CS GROUP are only analysed in Section 3 as the baseline of the APPRAISE platform in which to converge all the information collected and transferred by the different tools. More specifically the following 3 tools represent the basis of the platform as a whole:

- Cyber-secure context information and intelligence management and sharing.
- Intelligent Digital Twin-based Hypervision and Operation Management System (DITHO).
- AI augmented decision support.

Technology	Technology developer	Initial TRL	Target TRL
Novel tools for real-time early detection of security threats in public spaces			
Detection of threat-related objects and people from visual data	ATK	TRL 5	TRL 7
Video-based event and anomaly detection	ATK	TRL 5	TRL 7
Drone-based wide area mapping & surveillance	ASTRIAL	TRL 5	TRL 7
Relevant sound detection	CEA/ASTRIAL	TRL 4	TRL 6
CBRN threat detection	CEA	TRL 4	TRL 6
Hostile UAV threat detection	CS	TRL5	TRL 7
Crowd sensing and human sensors	INOV	TRL 5	TRL 7
Real-time crowd dynamics analysis	LINKS	TRL 4	TRL 7
Detection of cyber-attacks on surveillance system	ITTI	TRL 4	TRL 6
Actionable intelligence for proactive security			

Technology	Technology developer	Initial TRL	Target TRL
Advanced stream data analytics for early warning	ENG	TRL 5	TRL 7
Mobility for situational awareness	ALCHERA	TRL 4	TRL 7
Threat intelligence & real-time risk analysis	ENG	TRL 5	TRL 7
Event evolution prediction	CERTH	TRL 4	TRL 7
Geo-spatial intelligence	ASTRIAL	TRL 5	TRL 7
Risk-based surveillance attention	ENG	TRL 4	TRL 7
Internet content analysis tools			
Monitoring of criminal intent through online textual content analysis	CENTRIC	TRL 5	TRL 7
Detection of terrorist activity indications in multimedia content	VICOM	TRL 5	TRL 7
Identification of relevant people and criminal groups from online contents	LINKS	TRL 4	TRL 7
Context-based risk assessment of soft targets	ENG	TRL 5	TRL 7
Public-Private interoperability and collaboration services			
Context information integration and harmonization	ENG	TRL 6	TRL 8
Cyber-secure context information and intelligence management and sharing	CS	TRL 5	TRL 7
Tools for communication with the crowd	INOV	TRL 5	TRL 7
AR tools for on-site situational awareness and collaborative training	HOLO	TRL 5	TRL 7
Distributed collaborative improvement of situational awareness tools	INOV	TRL 4	TRL 7
Visualization and DSS services			
Intelligent Digital Twin-based Hypervision and Operation Management System (DITHO)	CS	TRL 6	TRL 8
AI augmented decision support	CS	TRL 5	TRL 7

3 MARKET ANALYSIS FOR THE APPRAISE PLATFORM

3.1 MARKET SITUATION AND TRENDS

Over the last years, terrorists and criminals have continuously attacked soft targets, thus maximising casualties and social impact. During different incidents, such as a shopping mall (Munich 2016), squares and streets (Paris 2015, Berlin 2016, Nice 2016, Stockholm 2017) and sports events (Boston 2013), the open nature of public venues and therefore their vulnerability has posed some challenges and shown a clear need to explore new means to better protect them.

As a result, European cities and the European society as a whole should explore new approaches to preserve the freedom of its citizens, while ensuring the safety of public spaces. The digitalisation of the society has made it more complex to protect soft targets, such as malls, stadiums, big events or expo centres. An integral security approach, combining cyber and physical protection means, as well as involving public and private security actors, is required. In this context, establishing a better operational collaboration among LEAs, private security personnel, and the citizens, along with using latest technology advances is essential.

Due to its holistic approach the APPRAISE platform, addresses simultaneously the physical and cyber security markets. The cybersecurity and physical security have for many years been addressed separately. Nevertheless, the advent of the Internet of Things (IoT) and Industrial Internet of Things (IIoT) has led to a configuration where the cyber and physical security are strongly interconnected. The US Cybersecurity and infrastructure security agency has issued a guide titled "Cybersecurity and Physical Security Convergence Guide" [1] analysing the benefits of a holistic security strategy aligning "cybersecurity and physical security functions with organizational priorities and business objectives." The guide identifies various benefits of the converged security functions vs siloed security functions. Despite the fact that the guide focuses on enterprises, the resulting benefits can be of huge added value when it comes to the protection of soft targets, e.g.

- Efficiency: connected physical security and cybersecurity functions reducing duplicative efforts and raises productivity.
- Strategic alignment: risk and threat management are fully aligned under a holistic strategy.
- Common goals: single security program under one set of shared practices and goals to secure cyber-physical infrastructure.

On European level ENISA has issued a report "Physical manipulation/damage/theft/loss" [2] focusing on ATM and POS related physical attacks. In this sector as well, there is a trend to move towards "hybrid cyber and physical security plans" acknowledging the link existing between cyber and physical security in the IoT era.

These studies and analysis clearly show that there is a raising awareness on the need to envisage security on cyber and physical levels as a whole, in order to ensure better protection for infrastructures and companies, as well as for citizens and soft targets. The focus of APPRAISE is therefore on two market segments considering them as tightly integrated, especially in the particular context of smart cities with innovative protection services for combined cyber-physical security.

The global Physical security market size is expected to grow at a CAGR of 6.5 from 2021 to 2030, meaning an increase from $104.6 billion in 2020 to $192.9 billion by 2030 [3]. On the other hand, the cybersecurity market was valued at $202.7 billion in 2022 and is expected to expand with a CAGR of 12,3% from 2023 to 2030 [4].

The drivers and barriers identified for the APPRAISE platform have been addressed in the table below with view to identify the man factors that will push forward or hinder the market penetration of the platform:

Factor	Drivers	Barriers
Political	- Growing need to efficiently protect soft targets against cyber and physical threats. - Will to better prevent, manage and learn from terrorist attacks - Rise in concerns about public safety and key infrastructure. - Increased awareness and need to collaborate with public and private security actors, including cross-border	- Existent regulations - Fear of the perception of a comprehensive and modular platform. - Reluctance and mistrust when it comes to sharing information with private security. - Reluctance and regulatory barriers when it comes to sharing information across border.
Economic	A single modular and flexible platform compatible with legacy systems.	Costs related to installation, maintenance and training of a new tool in comparison to existing ones.
Social	- Demand of increased security during social public gatherings. - Adaptability of the modular APPRAISE platform to the different social and cultural constraints of each country.	- Negative social perception in case of failure - Negative perception and reluctance when it comes to data collection and surveillance tools
Technological	Mobile, easily deployable and cybersecure solution enabling a combined and holistic approach to simultaneously protect soft targets from cyber and physical attacks	Technological barriers and readiness to adopt state-of-the-art technologies.
Legal	Regulations and need to protect soft targets (or other infrastructures)	Legal barriers related to GDPR, ethical and legal constraints when it comes to personal data collection.
Environmental		Concerns about carbon footprint and sustainability related to data collection, processing, storage and transfer.

3.2 MARKET SIZE AND SEGMENTATION

MARKET SEGMENTS, VOLUME AND PATTERN

On the global security market the APPRAISE platform will target the following market segments:

Market segment	Volume	Pattern (emerging/growing)
Cybersecurity market	$202.7 billion in 2022	Steadily growing

Market segment	Volume	Pattern (emerging/growing)
Physical security	$104.6 billion (2020) → $192.9 billion (2030)	stable
Global smart cities market	$511.6 billion (2022) → $1024.4 billion (2027) [5]	Growing
Cyber and physical security	N/A	Emerging

CUSTOMERS

The typical customers for the APPRAISE platform would be LEAs, security operators, as well as companies/organisations supporting or managing soft targets in urban-metropolitan areas.

The typical customer of the APPRAISE system would have a complex infrastructure to manage, high productivity demand and both budget and personnel constraints. The size and specificities of the site to protect, combined with the constantly increasing complexity of threats and risks make it impossible to perform manual/human monitoring of all potential threat sources increasing the direct benefits of and automation and decision support capabilities provided by the APPRAISE platform.

STAKEHOLDERS

In order to build and prepare the exploitation of the APPRAISE platform addressing multiple market segments, as well as different public and private security operators a multi-layered stakeholder audience is targeted.

At the start of the project the following stakeholders have been identified in D10.1 (Dissemination and communication plan):

- LEAs, Intelligence Services, Cybersecurity and Cyberterrorism units
- Legislative authorities and policy makers
- ICT Private Sector and technology providers
- Media, Civil Society and General Public
- Academic and Research Community
- EC, National, Regional and Local Decision-Making Bodies

PRIORITY MARKETS

The priority market for the APPRAISE platform is the European market, starting with the countries involved in the project. Other potential markets can be in North America and Asia.

3.3 COMPETITORS

The current urban security market lacks a holistic solution that meets both LEA and private security agents needs providing protecting against criminal and terrorist attacks. Actors like Anixter International provide offerings for smart cities and urban infrastructures security and point out the rising concern and need to take into account the Cyber and Physical dimension, yet their products do not cover the same needs as the ones addressed by the APPRAISE platform. The main competitors' landscape is complemented by Honeywell and Johnson Control, focus are public/urban safety, border security, energy sector, medical sector, home/private sector.

Furthermore, additional relevant competitors are: Motorola Solutions a global leader in Public Safety markets, Abbott Informatics, DFLABS, IBM, IntelliChoice, and Wynyard Group. Other prominent vendors in the market are: 911 Tech, Alert Public Safety Solutions, Blackthorn GRC, CODY Systems,

Competitive Edge Software, Crimestar Corporation, CSE, DataDriven, Digital Design Group, Diverse Computing, Envisage Technologies, ESRI, Harris Systems USA, Larimore Associates, Numerica Corporation, PTS Solutions, Saltus Technologies, SysTools Software, and Zuercher Technologies.

3.4 PARTNERS AND PROVIDERS

The APPRAISE platform is modular and dependent on the offerings of the different partners. It can be adapted to the needs of the public or private security client by including technologies relevant for the implementation environment.

Partnerships with different APPRAISE beneficiaries or providers of existing legacy systems used by the potential clients are to be considered and envisaged.

3.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Alignment with EU strategies and challenges set up in the Action plan to support the protection of public spaces • Strong innovations brought to urban security • Combined solutions developed by top rank European business, research and user partners. • High transversal networking potential • Modular, scalable and holistic approach • Modular tools leveraging open source.	• Different ambitions among partners • Some APPRAISE components not ready for the market • Complexity to integrate many different components • Hard to address very large organisations as customers • APPRAISE unfamiliar to customers (business reputation) • Leadership and IPR management after project end.

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Addressing a sector (soft target cyber/physical security) with strong investments and critical for urban economy • Consulting opportunities • Improving effectiveness of human protection • Many assets exploitable as ‘stand-alone’ • Address new domains in C/P protection • Ensured continuous research and innovation	• Competition with other similar projects/products. • Advancements of criminals/terrorists in the technological field • Reluctance to pay for the APPRAISE platform and services. • Resistance to adopt APPRAISE solution by other cities/countries • Retreat of partners after the project

• Create best practices and contribute to policies and standards • Improving perception of such tools through communication, dissemination and pilot activities. • Collect societal acceptance data through questionnaires and work on mitigating main SELP concerns	• IPR management • Similar projects/initiatives perceived as equivalent.

4 MARKET ANALYSIS FOR THE APPRAISE COMPONENTS

4.1 NOVEL TOOLS FOR REAL-TIME EARLY DETECTION OF SECURITY THREATS IN PUBLIC SPACES

4.1.1 DETECTION OF THREAT-RELATED OBJECTS AND PEOPLE FROM VISUAL DATA

4.1.1.1 MARKET SITUATION AND TRENDS

A threat is a "*possible source of harm and danger*" and the related condition of putting people in danger or at risk. The origin of the threat might come from a human being or even an autonomous computer program. Therefore, the goal of a **threat detection system** is to rapidly detect the threat while ensuring the security and the safety of the persons/organizations involved. The term security implies a combination of integrity and confidentiality that a threat detection system must indeed guarantee. At the basis of the global rise of threat detection systems is the increasing incidence of terrorist attacks, which increasingly occurred in the past few years, and the subsequent need of increasing protection of public infrastructures (e.g., naval port, railways stations, airports etc) and private premises (e.g., banks, malls, etc). The table below summarises drivers and barriers associated to the threat detection system market:

Factor	Drivers	Barriers
Political	Geopolitical instabilities, increased terrorist attacks	
Economic		High costs of threat detection systems; operational response vs. real demand
Social	Demand of increased security during social public gatherings (especially in large scale events); possibility to detect spreading disease (e.g., COVID-19)	Negative social perception in case of failure
Technological	Requests to upgrade existing technologies to ensure a faster and more reliable detection (including AI technologies); increased request of biometric recognition systems	Any existent technology limitation (e.g., avoiding black box of artificial intelligence)
Legal	Regulations (government-based) for security devices	Possible privacy breach, Integrity, and confidentiality concerns (e.g., biometric recognition)
Environmental	Rapid and safe detection/inactivation of threats of nuclear, radiological, viral, bacteriological, explosive nature	

4.1.1.2 MARKET SIZE AND SEGMENTATION

The threat detection systems can widely include explosive detection, suspect luggage detection, biometric recognition, etc. Therefore, the **market segmentation** will follow the nature of the application, products, and geographical regions (e.g., emerging nations vs. industrialized nations). Based on these assumptions, the threat detection system market can be divided into e.g., video-surveillance, biometric recognition, radar, and dosimeter. Of these, the video-surveillance market is the dominant one with its installation into commercial, industrial, and public premises, to name a few.

The **identified customers** could be governments (both at the institutional and public defence levels), public sector and infrastructures (e.g., companies owing railway stations, airport, naval port, hospitals, universities), and private industries (large-scale logistics, malls, concert halls, etc.).

- policy makers (political/legal): any institution for GDPR and privacy protection e.g., Garante della privacy (Italy), European Court of Auditors, European data protection supervisor, any organization/company/industry adopting e.g., video surveillance systems must agree to a publicly-available system policy.
- volume of each market segment and its pattern: the global Threat Detection Systems market size was valued at USD 65711.61 million in 2021 and is expected to expand at a CAGR of 9.66% during the forecast period, reaching USD 114282.18 million by 2027 [5]. It is generally a growing market; however, the high costs of threat detection systems purchase may limit its widespread utilisation in multiple public sectors (e.g., in aviation and transport sectors). As for the segmented market, the video surveillance market was valued USD 42.94 billion in 2019 and is projected to reach USD 144.85 billion by 2027, with a 14.6% CAGR in 7-year timeframe [6]. For which the global biometrics market, the revenue in 2021 was of USD 27.97 billion, with an estimation of USD 74.42 billion by 2027 and a 17.5% CAGR between 2020 and 2027 [7].
- priority markets per countries/segments: the threat detection system market is expected to be highly lucrative in North America, Pacific Asia, and Europe. North America is currently investing in research and development activities, especially in the high-energy laser to lead that sector.

4.1.1.3 COMPETITORS

The threat detection system is a highly competitive market, due to the heterogeneity of players, integrated technologies and possible market applications.
The main direct competitors of threat detection systems are: Safran SA, Rapiscan Systems Inc, CheImage Sensor System, to name a few. While competitors in the video surveillance market are Bosch, Hikvision, Dahua, FLIR, VIVOTECK, Tiandy, Hanwha Techwin, Ifinova, Uniview and Axis. These companies have been named the top-10 in the video surveillance market and together produced a revenue of $17.76 billion, or 85.5 percent of the $20.8 billion combine total in 2019 [8].
There are some features to take into consideration when choosing a video surveillance provider company, such as the specific software they provide (e.g., AI-guided recording, high resolution, audio support etc), the scalability of the products, the ease of installation and the application/sector they serve (e.g., crime prevention *vs.* evidence collection vs. public transports *vs*. law enforcement *vs*. explosive detection etc.). Therefore, not all the aforementioned companies can be easily exchanged as a provider in the market.
The video surveillance sector is regulated by standards and certification such as the ISO standard ISO 22311:2012 for societal security purposes [9], the ISO 30137 for the use of biometric in CCTV [10] and

the ISO/IES JTC 1/SC 42 for implementation of Artificial Intelligence [11]. Any other regulations published by the European Commission [12].

4.1.1.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Highly scalable. • Supports various types of hardware. • Different kinds/implementations of detection algorithms can be deployed and swapped easily (using Dynamic AI Server plugin system), without affecting the end user. • Usage of the service is provided through a secure and authenticated communication channel. • Robust and flexible licensing system.	• Custom protocol over TCP requires usage of SDK for integration. • Communication via network socket requires relatively high and consistent bandwidth. • HTTPs protocol (as an alternative to the custom protocol) is available but could use further development.

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
Could develop server-side SDK for third-party plugins providing detection algorithms.	Detection tasks are increasingly being deployed on-edge (e.g. in the cameras).

4.1.2 VIDEO-BASED EVENT AND ANOMALY DETECTION

4.1.2.1 MARKET SITUATION AND TRENDS

Anomaly detection software - often based on machine learning and deep learning (both branches of the artificial intelligence) - enhances the finding of rare events (e.g., outlier detection) or those observations (as unlabelled data points) that do not fit in the distribution and for that may pose a threat or a suspicion. The anomaly detection market has been fuelled by many different factors, explaining its growth in the recent years:

Factor	Drivers	Barriers
Political	Geopolitical instability; increased terrorist attacks (concerning also cyber security)	
Economic	Increasing economic threats, cyber espionage, digital payments	

Factor	Drivers	Barriers
Social	Health monitoring; intrusion detection; increasing number of connected devices; remote working; pandemic restrictions	
Technological	Overcoming the “black box” concept associated to AI	Lack of technical expertise; other open-source alternatives
Legal		Identity theft; Integrity, and confidentiality concerns
Environmental		

4.1.2.2 MARKET SIZE AND SEGMENTATION

The anomaly detection market is usually divided into market segments by types (solutions vs. services), deployment (cloud vs. on-premises), end-user industry (IT, healthcare, manufacturing, banking/financial/insurance BSFI) and geography.

The main customers according to the segments might be private banks, insurance and financial companies or groups, public or private hospitals and clinics, public sector and infrastructures (e.g., railway stations, airport, naval port, schools, universities). As the anomaly detection could be coupled with other systems of data acquisition and collection, such as video surveillance monitor, the identified list of customers may increase.

- policy makers (political/legal): any institution for GDPR and privacy protection e.g., Garante della privacy (Italy), European Court of Auditors, European data protection supervisor; ISO standards
- volume of each market segment and its pattern: anomaly Detection Market size was valued at USD 3.43 Billion in 2020 and is projected to reach USD 9.58 Billion by 2028, growing at a CAGR of 16.65% from 2021 to 2028.
- priority markets per countries/segments: the anomaly detection market is expected to be highly lucrative in North America, Pacific Asia, and Europe. North America has currently the largest share in the market (e.g., home of the multinational Cisco System), while Pacific Asia (especially China) is expected to growth rapidly in the next years.

4.1.2.3 COMPETITORS

The anomaly detection market has been evaluated as an intermediate competitive market (in between from the fragmented and highly competitive and the consolidated markets) [13], with the potential high rivalry amongst players.
The key market players are IBM, Cisco Systems, SAS institute, Gurucul, Verint Systems Inc and Symantec Corporation.
The market has not been saturated yet and the top players are generally a big name in the IT world. The change in providers might be allowed based on the offers and the features requested by the customer, the price and the infrastructure (cloud vs. server). However, thanks to strategic partnerships

and acquisition, the companies in the market tend to maintain their primacy to provide the optimal products and solutions to their customers.
The ISO/IES JTC 1/SC 42 for implementation of Artificial Intelligence [11]. Any other regulations published by the European Commission [12]. In case of association with video surveillance systems, the ISO standard ISO 22311:2012 for societal security purposes [9], the ISO 30137 for the use of biometric in CCTV [10].

4.1.2.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Can detect a large variety of events and anomalies • Configuration UI is comprehensive and entirely HTML (accessible with a browser without requiring any proprietary client software) • Thanks to the Dynamic AI Server architecture, image processing is decoupled from the event/anomaly detection, allowing for the two operations to run on different machines; a single Dynamic AI Server can serve multiple analysis, or vice versa • Can use metadata produced by some cameras (e.g. ONVIF tracks, BOSCH metadata) • Easy to integrate with third party systems, thanks to a plugin-based notification system	• Analytics modules (e.g. AiVu Smart Modules) are integrated in the AiVu NVR, requiring an entire NVR to be deployed to run analytics

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Integrate third-party data to apply some combined analytics • As cost of computation keeps getting lower, more advanced deep-learning applications can be developed and offered	• Significant competition in a fast-changing market, with on-edge computing increasing functionalities every year

4.1.3 DRONE-BASED WIDE AREA MAPPING & SURVEILLANCE

4.1.3.1 MARKET SITUATION AND TRENDS

The drone industry serving sectors such as public safety, critical infrastructure protection e.g., oil and gas, harbours, energy providers is growing in the past years at an annual rate up to 20% is specific sectors.

The reason for this growth is that drone technology offers far more than normal surveillance. It offers a safer and economical way to access and integrate data, critical for the site safety and efficiency.

The threat of attacks on sites critical to national, global infrastructure and events/sites with crowded people is a reality.

Drones provide a mobile and rapidly deployable solution to extend surveillance. They also provide a way to access and monitor areas without having to dedicate or even risk human resources.

Another growing sector in the drone industry is the possibility of detailed 2D and 3D-area mapping. Drones provide area-based, up-to-date, detailed and accurate 2D and 3D data that can be used as a basis for planning safety and providing a better and more detailed situational awareness picture on site during incidents.

Factor	Drivers	Barriers
Political	Increasing attacks on critical infrastructures and events/sites with crowded people	
Economic	Lack of personnel in the security sector. Low costs compared to video images from helicopters. Mobile solution which can be used for different sites/events	
Social	Increasing demand for security during public events	
Technological	Mobile Solution. Quick deployment.	Drone Batterie last up to 40-50 minutes
Legal		Impact on private life and property.
Environmental		Battery Recycling

4.1.3.2 MARKET SIZE AND SEGMENTATION

- Public safety, critical infrastructure protection e.g., oil and gas, harbours, energy providers, airports, Sport Venue Organizations
- In addition, identify the market stakeholders:
    - policy makers (political/legal): All EU institution for privacy protection. Aviation authorities responsible for drone flights

- The market is projected to grow from USD 142.0 million in 2021 to USD 476.5 million in 2028 at a CAGR of 18.9% in the 2021-2028 period
- Priority markets are the European Union, North America and the Asian Market

4.1.3.3 COMPETITORS

Identified market competitors:

- National System integrators with their Subcontractors in the Public Safety Market
- Usually not because the drone surveillance System is part of a bigger Security System
- Legal barriers are existing, depending on the countries and usually the non-existing implementation experience if you are new in the market

4.1.3.4 PARTNERS AND PROVIDERS

The Hardware is depending completely on other providers, as well as some software components like flight route planning, 3D- mapping.

4.1.3.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Mobile Solution • Quick Deployment • More detailed situational Awareness due to 3D-Mapping • Large scale Automatic Abnormal behaviour of people and vehicles and alarm triggering in crowded places	• Battery duration during flights is max. 40-50 minutes. Needs some time to replace with new batteries

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Gives the Police and Security Forces an added value for their Fleet of Drones • Easy integration in Third-Party Systems	• Fast Development in the Drone Market with yearly updates in new applications

4.1.4 RELEVANT SOUND DETECTION

4.1.4.1 MARKET SITUATION AND TRENDS

Sound detection is used in different fields of audio surveillance. For security application sound detection could be useful to have a speech recognition, an embedded system with less data recorded as video one, or when the video couldn't be used (special room, low lights, smoke ...).

Factor	Drivers	Barriers
Political	In case of hostage taking, if the system is bidirectional, transaction could be fluent	Audio surveillance as any surveillance system should prove its relevance to be adopted by end-users.
Economic	Audio surveillance is less expensive than video one	Audio surveillance is a technological system requiring some experts in order to be used correctly or automated treatment and interfaces
Social	Audio surveillance, as it is less intrusive, could be more widely accepted like continuous video monitoring	Audio surveillance should be strictly used to be accepted (example Alexa) and avoid spying
Technological	System less complex for automation than video	System less informative than video in normal conditions of light
Legal	As audio surveillance is less intrusive, legal aspects are simplified.	Speech recognition could be done and privacy rules should be respected
Environmental	Audio surveillance is less expensive for components as video ones and data exchanged are also more frugal	To have a relevant system in outdoor context some equipment is needed (cables or antenna, masts...)

4.1.4.2 MARKET SIZE AND SEGMENTATION

- Audio surveillance is dedicated to two main fields: security (to monitor any place continuously in indoor or outdoor context) and safety (home support for people).
- Here, the one developed is dedicated to security application due to the algorithm to detect abnormal sound (gunshot, explosion...). So, the stakeholders are security agencies or building's security teams. The system is not easily reconfigurable to be useful for police deployment in not known place (triangulation aspect, noisy environment...).

4.1.4.3 COMPETITORS

- For any surveillance system, interoperability with different providers is more or less easy according to the privacy (open API could allow providers change easier than another).
- For new entrants, the barriers are technical (interconnexion to existing solution) rather than legal or political because the system is dedicated to security teams.

4.1.4.4 PARTNERS AND PROVIDERS

- The system is provided by ASTRIAL and isn't an open-source service for security reason. The system is built with specific microphones. Any change needs ASTRIAL intervention to ensure that new microphones are compatible with the system (e.g. angle, precision).

4.1.4.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• System successfully used in different cases • Reconfigurable system for another abnormal sound	• Reconfiguration not automated • System not mobile (system should be put in place durably) • System for specific place or environment where video could not function

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• To have a bidirectional information in case of hostage (bidirectional information has to be developed in that case, not done for APPRAISE project) • Less expensive, more discreet, less intrusive	• Video surveillance system • Less informative

4.1.5 CBRN THREAT DETECTION

4.1.5.1 MARKET SITUATION AND TRENDS

RN malevolent acts are now a preoccupation for homeland security teams even if these attacks are rare according to the difficulties to have access to NR elements. So, the market focuses more on RN surveillance of specific sites: RN recycling plants, RN production factories, RN storage places, border control, etc.). But some tools, as the ones deployed in airport, could be useful to ensure security in large event.

Factor	Drivers	Barriers
Political	Security reinforcement.	

Factor	Drivers	Barriers
Economic	Homeland security (in case on NR contamination, remediation needs specific infrastructures).	This additional tool could be found expensive regarding to the frequency of the event.
Social	NR contamination has deep social impact (confidence, health...)	
Technological	System is non-intrusive;	System needs to have a non-mobile object/person to acquire NR data with a convenient distance to be relevant (sensors should be put in entrances)
Legal		
Environmental	Early detection could avoid a large contamination	System needs resources to be developed/built etc

4.1.5.2 MARKET SIZE AND SEGMENTATION

The Market for RN detection focuses on specific plants dealing with RN (plants, storage...) or for toll control. The market segments are well defined so the stakeholders too.
The Market is in extension because sensors are more affordable and RN production and storage are growing. Moreover, now some dismantling actions are in progress in the oldest nuclear plants. So, radioprotection is needed to ensure the safety.

4.1.5.3 COMPETITORS

The NR market is a niche market. However, since the Fukushima events, a lot of research centres worldwide worked on gamma imaging solutions. This led to a large worldwide offer (H3D – US -, ASTROCAM – Japan -, SPIDIX, NUVISION, IPIX – France). New entrants have to master NR physic and have NR source available: this point is strictly controlled by any country.
For now, Nanopix system, the basis proposed in APPRAISE is a co-development between CEA and ORANO. It is the world smallest gamma camera and this advance makes it a key feature in the worldwide range of developed systems.

4.1.5.4 PARTNERS AND PROVIDERS

The gamma imaging system relies on a development carried out in the frame of an international collaboration lead by CERN and of which CEA is co-founder. The detection brick is therefore dependent on CERN and the semiconductor crystal from a European provider in the field.

4.1.5.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Gamma camera is a fruitful solution designed by CEA and ORANO since many years and continuously improved. • The Nanopix (the last generation of gamma camera) is designed to be less voluminous to be involved in on-the-fly deployments	• Gamma camera need to have convenient distance to detect NR threats. • Some fixation point and connection are needed to use gamma camera, moreover a deported PC collects information and algorithms to return the augmented picture

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Market in progress to secure new locations	• Gamma camera is still expensive according to the threat frequency in the public event but not according to the health consequences of a contamination • A lot of competitors are currently emerging worldwide even if form factor is still a strength

4.1.6 HOSTILE UAV THREAT DETECTION

4.1.6.1 MARKET SITUATION AND TRENDS

The rapid development of drone sales has lowered the economic threshold for their acquisition. From a law enforcement perspective, increased drone ownership drives the need for developing and procuring C-UAS capabilities.

Events such as the disruption caused by rogue drones at Gatwick airport over the 2018 Christmas period demonstrate the need for law enforcement agencies or private operators to be able to deploy effective C-UAS capabilities. Similar events in other countries have triggered C-UAS procurements, and there is now a wider awareness across governments, civil security forces, law enforcement agencies, and private operators that deploying C-UAS solutions is essential to ensure security of their assets, official buildings/sites and populations.

The table below proposes a high-level analysis of the C-UAS market drivers and barriers:

Factor	Drivers	Barriers
Political	European strategy (cf. European Commission Drone Strategy) Organization of major events (e.g. Olympic games)	Applicable regulations Grey areas in terms of responsibility between private actors and

Factor	Drivers	Barriers
		police/army forces (e.g. for sensitive site protection)
Economic	Potential financial impact/loss of revenue/reputation could be extremely significant in case of UAS incident/attack	Significant budgets required for C-UAS systems
Social	Need to protect people & soft targets	Difficult topic yet to be addressed with populations, the awareness of the issues raised by UAS amongst general population remains low
Technological	Significant technological improvement on C-UAS technologies over the past few years, good performances at reduced costs now available	Rapid growth of the UAS R&D: C-UAS solutions always need to catch up with the latest UAS innovations (endurance, agility, autonomy, etc.)
Legal	There could be in the future some obligation for critical sites to be equipped with C-UAS systems (not yet formally the case however)	Regulations
Environmental	N/A	Choice of equipment to comply with the environmental standards

4.1.6.2 MARKET SIZE AND SEGMENTATION

MARKET SEGMENTS AND TYPE OF CUSTOMERS

The C-UAS market is growing rapidly, there are a number of market analysis studies available, as an example we can mention the figures from Visiongain published a few months ago ("Counter-UAV 2022-2032"), valuing the global counter-UAV market at US$1,087 million in 2021 and projecting its growth at a CAGR of 29.0% during the forecast period 2022-2032.

The C-UAS market is quite large as many users/activities are concerned with potential security issues. We can mention the following types of potential customers:

- Civil security: protection of sites, in homeland or overseas
- Law enforcement agencies: public protection (events, large gatherings)
- Private assets protection (industrial sites, airports, stadiums, etc.), VIP protection

The market segments are quite wide as many use cases can be envisaged. We can mention:

- Defence
- Governments
- Homeland Security
- Private Security
- Airports

- Sports Teams and Stadiums
- Amusement Parks
- Utilities
- Chemical Manufacturing
- Oil & Gas Facilities
- Universities, research facilities
- Etc.

MARKET STAKEHOLDERS

In addition of the typically expected stakeholders like media, who often voice incidents caused by UAS, and sometimes rely on websites/marketing material issued by the C-UAS industrials, we can mention specifically for C-UAS:

- **Policy makers (political/legal)**: the massive use of drones raised the need for C-UAS solutions well before the legal basis to use such solutions was up-to-date, things have now been somehow cleared at national level but some major issues still remain, in particular for using effectors, as of today this remains a LEA prerogative (if even authorized). In this respect we can mention 'A Drone Strategy 2.0 for a Smart and Sustainable Unmanned Aircraft Eco-System in Europe', issued by the European Commission on 29 November 2022, which highlights the following actions:
    - Flagship action 17: The Commission intends to adopt a counter-drone (C-UAS) package [outlining the EU's future policy in this field]
    - Flagship action 18: The Commission intends to adopt an amendment to the aviation security rules aiming to ensure that aviation authorities and airports increase their resilience when faced with the risks posed by drones
- **Prescribers**: some countries like UK have adopted a systemic testing approach for C-UAS by public actors with the ambition to understand the threat, the C-UAS solutions, influence legal and policy development, and ultimately provide guidance to support customers in selecting a suitable C-UAS solution.
    - The user guide edited in that respect by CPNI is intended to help critical infrastructure operators assessing their C-UAS needs [14].
    - The MoD, through the UAS Capability Development Centre (UASCDC), is more focused on SAPIENT, an interoperability standard developed within UK MoD, and currently being pushed as a NATO-candidate interoperability standard for C-UAS systems [15]:

  Other initiatives at European level also are being conducted to prescribe the future of C-UAS. We can mention the following on-going projects:
    - **Courageous**, a European project (ISF Police) aiming at defining standardized testing methodology to better assess the capabilities of the C-UAS systems. This project is entirely led by public/governmental entities, and C-UAS industrials will be invited to 3 trials aiming at validating the proposed standard
    - **JEY-CUAS**, a European project (EDIDP) aiming at defining the future European C-UAS capability. It is expected that this C-UAS capability shall be modular, scalable, evolutive, with standardized internal and external interfaces

Finally, we can mention NATO, which also aims at defining applicable interoperability standards that could apply to all NATO allies. This standards are both internal and external to C-UAS systems, and the initial assessment of candidate standards is being conducted through TIE (Technical Interoperability Exercise) held by NCIA, already held in 2021 and 2022.

VOLUME AND PATTERN OF THE MARKET

We can mention here figures from a market analysis by Fact.MR, a market research and competitive intelligence provider, issued in June 2022. While detailed figures have a relative importance, the expected trends for C-UAS market are impressive:

- Global anti-drone market poised to expand at CAGR of 20.9% reaching valuation of US$ 7.4 billion by 2032.
- **Europe** is likely to be **most attractive regional market** and is projected to utilize more than US$ 2 billion value of anti-drones by 2032.
- **North American** region expected to register a **CAGR of 19.2%** over the forecast period to be valued at **US$ 1.7 billion by 2032-end**.
- By end user**, civil security** likely to account for **1/3 revenue share** and create an absolute $ opportunity of US$ 2.4 billion over assessment period.
- 1 km – 4 kms anti-drones projected to grow 8.2X by value, while 4 kms – 25 kms drones to grow 6.7X during the forecast period.

PRIORITY MARKETS

From a civil security perspective, European market seems to be a priority for European C-UAS providers.

4.1.6.3 COMPETITORS

The C-UAS market has emerged in 2015 and has become very competitive ever since. There are now hundreds of companies proposing C-UAS solutions, either as sensor/effector manufacturers (most common) or as system integrators. We can however already observe that some of the early solutions have now disappeared, probably consecutive to the higher level of expectations that the Customers can have based on a better knowledge of the market and achievable performances.

COMPETITORS ANALYSIS

The C-UAS market is currently extremely competitive, however there are more sensor/effector manufacturers than system integrators. We can mention a few here:

Competitor	Country	Strength, added value
CS GROUP	France	Strategic contracts with French Army: MILAD, PARADE, SCCOA, etc. Several C-UAS systems operational since 2016.
SRC, INC	US	Numerous programs with the US Army: Silent Archer Counter UAS Technology, Counter RCIED Electronic Warfare (CREW) Duke system, and LCMR counterfire radars
Dedrone	US	Low-cost solution but only efficient against piloted commercial drones
Elbit	Israel	Strategic partnerships worldwide, efficient marketing strategy
Indra	Spain	Ability to manage large programs

ABILITY TO CHANGE PROVIDERS ON THE C-UAS MARKET

This topic is currently under scrutiny, as several early Customers have faced the impossibility to upgrade their C-UAS systems, particularly when the C-UAS system is sold directly by the equipment manufacturer (as opposed to a system integrator). In order to address this issue, but also the generic need for C-UAS systems to be scalable and evolutive over time with the ability to integrate new relevant technologies as they become available, some initiatives about C-UAS interoperability standards have been launched. Interoperability works addresses both internal and external interfaces (e.g. standard interface for a C-UAS sensor to communicate with a C-UAS C2, or standard interfaces between a C-UAS C2 and external systems). We can mention the following projects or working groups, to which CS GROUP actively participates:

- NCIA TIE (Technical Interoperability Exercise): These exercises, already held in 2021 and 2022, aim at defining future NATO standards for C-UAS interoperability. Candidate standards are SAPIENT (internal interoperability), ASTERIX and Link-16 (external interoperability). CS GROUP participates as Test Lead for Link-16 thanks to its knowledge and experience in both C-UAS and tactical data links
- Eurocae's C-UAS Working group (WG-115). This working group, jointly conducted with RTCA, aims at defining applicable standards for C-UAS systems in airport environments. CS GROUP has been elected the chairman of the group
- JEY-CUAS: This European project (EDIDP) started in November 2021, led by a consortium of 40+ European C-UAS actors, aims at defining the future European C-UAS system. This includes the generic architecture concept, as well as internal and external interfaces

SUBSTITUTES

The C-UAS market is still quite recent, and substitutes are not yet emerging. We could envisage in the future that a "C-UAS as a service" offer, based on a downloadable application and using a network of sensors deployed over a region/town/area could be offered as opposed to individual solutions/services, but such a deployment would need to get authorized.

BARRIERS FOR NEW ENTRANTS

The C-UAS market doesn't have strong barriers as such, however we can observe the following:

- UAS detection can be very complicated and thus require a significant volume of technical trials to test/tune/validate technical solutions. Early players in that market can rely on years of experience which can prove very precious
- Some technologies used in C-UAS solutions, can be classified as either dual use or fall under export control regulations, which can bring some constraints to address specific markets
- The legal framework applicable to C-UAS is still in progress, some emerging technologies relevant to C-UAS can be against applicable regulations in some countries (e.g. some countries still don't allow jamming, and the current trend for spoofing technologies comes with its regulatory issues)

4.1.6.4 PARTNERS AND PROVIDERS

As a C-UAS system integrator, CS GROUP has always considered that it would bring more added value to its customers to integrate the most relevant sensors and effectors available on the market to its BOREADES solution, that managed to system intelligence through its proprietary C2 component. It also become more and more obvious that the only best to achieve the highest performances is to integrate and manage multiple technologies, that can then be fused thanks to (heterogeneous) multi-sensors data fusion.

BOREADES C-UAS solution will therefore never rely on or by dependent on a specific provider, which is still aligned with the initial product strategy for BOREADES.

However, the potential for technological partnerships is huge, we already have a number of technology partners, either from industry or from research/universities. We have tested and integrated in BOREADES a number of products, but with some others we have worked more deeper to upgrade the performances offered by that single sensor/effector in line with our overall system performances ambitions.

4.1.6.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	WEAKNESSES
• Better performing solutions • Operational experiences	• Regulations/standards still under development

EXTERNAL FACTORS	
OPPORTUNITIES	THREATS
• Awareness of the increasing need for C-UAS systems	• Available budget • Legal framework • UAS technologies R&D: constant need for C-UAS systems to keep up to date

4.1.7 CROWD SENSING AND HUMAN SENSORS

INOV as a research institute does not intend to explore commercially the crowdsensing application that is currently being developed in the scope of the APPRAISE project. INOV is mainly interested in exploring and applying state of the art technologies and to contribute to solutions that can help monitoring and securing soft targets with the main focus on implementing successfully the APPRAISE pilots. Nevertheless, INOV is fully available to give technical support within its area of expertise (mainly on implementing machine learning algorithms and techniques) to any partner that intends to reach the market and explore commercially their solution.

4.1.8 REAL-TIME CROWD DYNAMICS ANALYSIS

4.1.8.1 MARKET SITUATION AND TRENDS

Crowd management and monitoring are difficult tasks for police and defence departments, as well as governments, during large events. In such cases, the integration of innovative surveillance systems with video analysis capabilities provides end-users with automatic monitoring capabilities and near real-time situational alerts.

Thanks to the use of recent AI algorithms, video analytics systems are capable to process digital video streams, implementing several security-related functions, including crowd dynamic analysis. The adoption of such is accelerating due to the ability to detect real-time behaviour and actions and to provide end-users with insights and alerts. Rising security and safety concerns are expected to drive market expansion.

The demand for video analytics systems is expected to gain traction owing to rising smart cities initiatives across the EU countries and increasing investment to implement integrated video surveillance systems for governmental and law enforcement agencies, banking & financial institutions, and others. Integrated video surveillance systems gain traction because they can offer reliability, cost-effectiveness, and high accuracy. Furthermore, the recent proliferation of analytics platform aimed to reduce crime rates through timely alerts about unusual or suspicious activity is expected to drive the market in the near future.

Factor	Drivers	Barriers
Political	European strategy	Applicable regulations Grey areas in terms of responsibility between private actors and police/army forces (e.g. for sensitive site protection)
Economic	Increasing demand for Crowd Analytic tools in the security market State-of-the-Art (SoTA) advanced enough to be used easily	Significant budgets required for cameras, installation, and processing power
Social	People safety & soft targets	Privacy concerns related to misuse of the tool
Technological	Significant technological improvement on SoTA of deep learning models over the past few years.	Quite disruptive market, higher resolution cameras, vision on difficult situations (low light conditions, transmission compression, …)
Legal	Safety in public spaces needed to organize events	Privacy concerns
Environmental	N/A	N/A

4.1.8.2 MARKET SIZE AND SEGMENTATION

The global video analytics market size was valued at USD 5.32 billion in 2021. The market is projected to grow from USD 6.35 billion in 2022 to USD 28.37 billion by 2029, exhibiting a CAGR of 23.8% during the forecast period. The global COVID-19 pandemic has been unprecedented and staggering, with these solutions experiencing higher-than-anticipated demand across all regions compared to pre-pandemic levels. Based on recent market analysis, the global market had exhibited a rise of 17.9% in 2020 as compared to 2019 [16].

The increased availability of high-resolution cameras, e.g., 4K or 8K, enables organizations to get accurate and more sophisticated analyses of videos. The high-resolution videos help to identify and

analyse objects/people in the crowd, trigger alarms when certain conditions are met, filter and search videos, and draw insights from video metadata more accurately.

Apart from higher resolution, hardware capabilities are evolving, offering enhanced vision angle and better technological compatibility, which increases the adoption of high definition (HD) cameras across the security industry. Besides, increased image resolution enables superior digital zoom capabilities to enhance long-distance vision, thus allowing to analyse people's and crowds' behaviour, and vehicles movements more accurately.

4.1.8.3 COMPETITORS

The major players in the market are Honeywell International Inc., Robert Bosch GmbH, Axis Communication AB, HIKVISION, and IBM Corporation, among others. They are concentrating on creating intelligent video analytics solutions using cutting-edge technology such as advanced AI algorithms aimed at object and people identification and classification.
Openpath, Inc. announced an integration partnership with Cisco Meraki to create a new Video Management System (VMS). Cisco Meraki's cloud-based technology will be combined with Openpath's access control capabilities and smart camera surveillance that provides data and analytics that allow users to make better business decisions. Integrating security would be easier due to an all-in-one security platform that can handle both video and access management.

Honeywell Building Technologies is working with the Airport Innovation Lab at San Diego International Airport (SAN) to examine the application of advanced video analytics technology for improved airport safety and health. Through early summer 2021, Honeywell's analytics technology would be examined, tested, and developed in a real-world airport setting at San Diego.

Robert Bosch GmbH released the first cameras built on their open camera platform Inteox, beginning through the MIC inteox 7100i. They are compatible with the Security & Safety Things (S&ST) Application Store owing to the Open Security & Safety Alliance (OSSA) Technology Stack for video security equipment. Neural network-based analytics integrated video cameras, supporting predictive solutions with ML, high-quality imagery, sturdy housing, and third-party software programs for customized applications are among the features of the cameras.

Axis Communications launched Axis Object Analysis, which can recognize and identify humans and vehicles. Parking lots, public buildings, and warehouses are ideal for the AI-based solution. False alarms such as shadow movement, minor object movement, and so on are suppressed by the intelligent technology that powers it.

4.1.8.4 PARTNERS AND PROVIDERS

The natural partner for the technological transfer of LINKS solution is ATK (project partner). LINKS has good relationship with start-ups, in particular with Water View [17] that could be a good partner if it will include the security market in the company medium and long-term strategy. Concerning camera providers, since the system uses generic cameras, any is valid. With respect to the infrastructure, the only requirement is to have a VM with a GPU capable of programmable computation, where viable commercial solutions are mainly NVIDIA GPUs (CUDA) or Apple Silicon SoC (Core ML).

4.1.8.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Ability to work in different conditions and environments, ability to provide useful overall information and help the decision making.	• Scalability to large number of cameras due to computational cost. Limited automatization of the setup, which requires some human intervention for each camera (homographic correction). • People detection and tracking is not accurate in really crowded situations and when subjects are distant with respect to the observation point (camera).

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Improvements of safety in public spaces thanks to automatic alerts. Improved knowledge on crowd behaviours in public spaces during large events.	• Privacy related concerns due to misuse of the product.

4.1.9 DETECTION OF CYBER-ATTACKS ON SURVEILLANCE SYSTEM

4.1.9.1 MARKET SITUATION AND TRENDS

Factor	Drivers	Barriers
Political	In addition to economically driven cyberattacks many European countries are now at risk of cyberwarfare due to the Russia-Ukraine conflict.	No significant barriers
Economic	Effective cybersecurity requires highly trained personnel, the process of network analysis is labour-intensive. Delegating some of the workload to AI is economically viable.	No significant barriers
Social	The societal recognition of the problems of cybersecurity is increasing and with it the interest in effective intrusion detection solutions	No significant barriers

Factor	Drivers	Barriers
Technological	AI-based technologies have received increasingly positive recognition and increasingly wider adaptation in the last decade	Data labelling can be costly
Legal	GDPR and privacy-related legislation invalidates the current NIDS paradigms like deep packet inspection	No significant barriers
Environmental	flow-based methods decrease the used bandwidth, which has positive impact on energy use	No significant barriers

4.1.9.2 MARKET SIZE AND SEGMENTATION

- Currently, the main economies and countries in Europe (Germany, France, U.K, Italy, and Spain) are the main targets of cyberattacks – just behind USA and Japan. The average annual costs are on the increase.
- It is reasonable to assume that the interest of the companies operating in Europe in effective solutions to counter cyberattacks will be on the rise, opening new market opportunities for the vendors of cybersecurity solutions.
- It is also reasonable to assume that the expenses dedicated to cybersecurity issues will rise in line with the number of cyberattacks and with the number of affected companies

4.1.9.3 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Privacy compliant by design: the **MaLNID** components set the privacy of the users at the centre of the development process to never infringe on the citizen rights • Innovative approach: the MaLNID component bridges the gap between technical and non-technical aspects, providing a comprehensive, user-friendly interface to an advanced AI-based detection system • Pragmatic approach: MaLNID provides clear goals, clear communication with the user and implements a sweet spot between tried and tested methods with	• Rapid evolution of cyber threats: the network intrusion detection landscape is an arms race • MaLNID is a network intrusion detection component, and handles network intrusions very effectively – however, cybersecurity is an enormous domain and with the level of knowledge of untrained personnel could lead to misunderstandings as to what the component is required to do (it is not a silver bullet against all types of cyberattacks)

leading edge innovations in network intrusion detection • Scalability-by-design by utilising scalable technologies	

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• **Improvement of cyber protection is a** European **priority:** • A multitude of **reports and studies (ENISA, ECSO, etc.)** points out **the need to increase cyber**defense, including against network intrusions • **GDPR and new regulations** firmly **require** • Implementations of measures **to protect the privacy of** citizens. • **Modularity and reusability** of the component **will** allow the adoption of the component by the wider audience	• Lack of understanding of the necessity for cybersecurity solutions • Insufficient motivation to increase cybersecurity measures before the organisation falls victim to a major cyberattack (cybersecurity is seen as vitamins not as aspirin) • Lack of adequate, trained cybersecurity personnel

4.2 ACTIONABLE INTELLIGENCE FOR PROACTIVE SECURITY

4.2.1 ADVANCED STREAM DATA ANALYTICS FOR EARLY WARNING

4.2.1.1 MARKET SITUATION AND TRENDS

The Advanced Stream Data Analytics for Early Warning is a tool that integrates and merges the information coming from various intelligence tools in order to create a situational picture of what is happening. It provides users with enhanced predictive analytic tools complementing user efforts for threat assessment and crime forecasting. The tool is able to make use of multimodal data in an effective consolidated manner. Innovation: aggregation of different information from different tools (mobility, threat intelligence, etc.)

Factor	Drivers	Barriers
Political	Local administrations, regional and national governments increasing attention to equip LEAs with tools for early warning, thus better prevention	
Economic	Increasing demand for Data Analytic tools in the security market	Recent worldwide crisis (COVID-19, Russia-Ukraine conflict, energy prices) has negative effects on public

Factor	Drivers	Barriers
	Tools easily deployed in other sectors, thus representing more exploitation opportunities	expenditures, thus less investments in technological tools
Social	Prevention tools are highly accepted by citizens and society to avoid incidents, casualties and people's fear.	Social acceptance of data analytics tools
Technological	Last advances in technology innovations (software & hardware) facilitate launch of cutting-edge innovative solutions	Increased and continuous competition of innovative solutions from highly specialized companies
Legal		Legal and ethical concerns in EU about GDPR protection.
Environmental		Concerns about carbon footprint and sustainability since data analytics tools require typically high processing high-power consumption

4.2.1.2 MARKET SIZE AND SEGMENTATION

The data analytics market is expected to reach $132.9 billion by 2026, compared to $23 billion in 2019, according to Market Research Future [18].

Growth is coming from many different industries, but it is primarily driven by internal business intelligence goals. The North American market is predicted to remain dominant, but the Asia-Pacific region is rising in its data analytics use and capabilities more quickly than other regions, with China at the front of the pack.

Key factors driving the global data analytics market are the widespread adoption of advanced technologies for business operations and the rising demand for data analytics for faster decision-making processes and cost reduction. The implementation of data analytics techniques improves the efficiency and productivity of business operations and strengthens the organizational workforce. Data analytical techniques help identify and fix the errors in data sets with the help of data filtration tools, which further improve the quality of data to benefit both consumers and institutions, including insurance firms, banks, and finance companies. These advantages are responsible for the exponential growth of the global data analytics market. In addition, the rising volume and complexity of data due to increasing mobile data traffic, increasing adoption and development of technologies like AI and IoT, and cloud computing traffic, are fuelling the growth of the global data analytics industry.

Geographically, the global data analytics industry has been segmented into North America, Europe, Asia Pacific, and the rest of the world. Europe held the second-largest position in 2019, estimated at USD 6,428.0 million; the market is expected to have a CAGR of 29.8% over the forecast period. The UK held the largest market share of 38.1% in 2019, with a market value of USD 2.447.8 million; it is expected to register a CAGR of 29.7% during the forecast period. Germany was the second-largest

market in 2019, estimated at USD 1,249.1 million; it is expected to have the highest CAGR of 28.2% over the forecast period [18].

4.2.1.3 COMPETITORS

With the presence of a large number of global and regional players, the global data analytics market is moderately fragmented and competitive. Market players are actively involved in technological advancement, geographic expansion, and mergers and acquisitions in order to retain their position in the international market.

The key players in the global data analytics market are: IBM Corporation (US), Microsoft (US), Oracle (US), SAP SE (Germany), Amazon Web Services, Inc. (US), Tableau Software, LLC. (US), SiSense Inc (US), Zoho Corporation Pvt. Ltd. (India), ThoughtSpot, Inc. (US), Mu Sigma (US), Looker Data Sciences, Inc. (US), Datameer, Inc. (US), Alteryx, Inc (US), Dell Inc. (US), and SAS Institute Inc. (US).

4.2.1.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Advanced information fusion from various intelligence tools	• Intricate nature of regulatory compliance, especially to data protection

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Various applications in other domains such as Disaster resilience, Border protection, SaR, and protection of critical infrastructures	• Exponential increase of the amount of data to be processed

4.2.2 MOBILITY FOR SITUATIONAL AWARENESS

4.2.2.1 MARKET SITUATION AND TRENDS

The target market is Highways Operators who operate the road network: both day-to-day and for major events. Depending on the geography, this target market is a combination of public and/or private organisations. The main market driver for this development is a trend towards uptake of AI-driven solutions which address a tangible outcome (such as congestion caused by broken-down vehicles).

Factor	Drivers	Barriers
Political	Investment in infrastructure (due to potential recessions), including	Sometimes slow-moving momentum

Factor	Drivers	Barriers
	smarter management of infrastructure	
Economic		
Social	Strong drivers around road users not wanting to be stuck in traffic	
Technological	Strong trend to use of technology (e.g. data-driven road management, smarter traffic lights), instead of more "traditional" physical interventions (e.g. new roads, more lanes)	Cultural and behavioural change, especially around use of new technology requires investment in each organisation, to unlock the value of the technology, but this is definitely surmountable - as demonstrated on multiple occasions
Legal	n/a - no PPI / GDPR data used in processing	n/a - no PPI / GDPR data used in processing
Environmental	Changing circumstances (climate, disease and resulting changes to patterns of life & travel) is making operators rethink many aspects of their operations - presenting an opportunity for positive change	

4.2.2.2 MARKET SIZE AND SEGMENTATION

MARKET SEGMENTS AND TYPE OF CUSTOMERS

- Road Operators, for example:
  - Public Sector - in Europe - and US - for example Local/Regional Authorities
  - Private Sector - in Europe - and US - for example Highways Operators and Private Concessions

MARKET STAKEHOLDERS

- Policy makers, particularly in relation to appetite for and regulation around Public-Private Partnerships to operate highways
- Media - particularly in their reaction to use of technology (sometimes positive, sometimes negative)

MARKET SEGMENT VOLUME AND PATTERN

- Public Sector is a £1.5 billion Total Addressable Market (Europe)
- Public Sector is a £2.5 billion Total Addressable Market (US)
- Private Sector is a £5 billion Total Addressable Market (Europe)
- Private Sector is a £5 billion Total Addressable Market (US)
- Infrastructure industry is stable. Use of technology in its operation is emerging and growing.

PRIORITY MARKETS

- UK
- Europe
- US

4.2.2.3 COMPETITORS

n/a - this is commercially sensitive

4.2.2.4 PARTNERS AND PROVIDERS

- No component providers - operators already have the deployed hardware necessary
- Cloud providers required - as cloud-based technology
- Potential partnerships with consultants who undertake a large amount of the work for operators
- Potential partnerships with operators, who often work on behalf of concessions (e.g. Cintra)

4.2.2.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Robust so can be depended on for incidents and other critical operations • Real-time for high value use cases • Built on a scalable platform for stronger, deeper integration into ecosystem	• Requires teams capable of responding to alerts and managing a network in response

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• A desire to maximise existing road space • A desire to draw on efficiencies from use of technology	• Resistance from road-users - especially in response to negative media coverage

4.2.3 THREAT INTELLIGENCE & REAL-TIME RISK ANALYSIS

4.2.3.1 MARKET SITUATION AND TRENDS

Threat intelligence in APPRAISE has a dual purpose: first, to analyse the data from the risk assessment to understand when a risk could turn into an accident (for example by applying in-depth content analysis to understand if it contains words that could incite hatred, violence, which give indications on how to create an attack, etc.); second important goal is to combine and merge the information coming from several sources in such a way as to create aggregated alerts that take into account the different analysis performed by the different sensors.

Innovation: the analysis of data from social media is something that is not very widespread in the various threat intelligence platforms, especially by applying deep learning techniques. Furthermore, the aggregation of information, again in the context of threat intelligence, would improve the overall performance of the system.

Factor	Drivers	Barriers
Political	Governments and decision makers increasing attention for intelligence and risk assessment to apprehend terrorists and prevent attacks before they happen	
Economic	Increasing demand for real-time risk analysis in the security market Tools easily deployed in other sectors, thus representing more exploitation opportunities	Recent worldwide crisis (COVID-19, Russia-Ukraine conflict, energy prices) has negative effects on public expenditures, thus less investments in technological tools
Social		Social acceptance of intelligence and risk-analysis tools because they typically use massive data
Technological	Last advances in technology innovations (software & hardware) facilitate launch of cutting-edge innovative solutions	Increased and continuous competition of innovative solutions from highly specialized companies
Legal		Legal and ethical concerns in EU about GDPR protection.
Environmental		Concerns about carbon footprint and sustainability since data analytics tools require typically high processing high-power consumption

4.2.3.2 MARKET SIZE AND SEGMENTATION

According to the **marketsandmarkets** [19] recent report, global threat intelligence market size is projected to grow from USD 11.6 billion in 2021 to USD 15.8 billion by 2026, at a Compound Annual Growth Rate (CAGR) of 6.5% during the forecast period. This growth is attributed to the R&D investments by governments and enterprises to develop robust threat intelligence solutions and

increase in the demand for professional and managed security services. The increasing venture capital funding and growing investments in threat intelligence to drive market growth.
This growth is attributed to the R&D investments by governments and enterprises to develop robust threat intelligence solutions and increase in the demand for professional and managed security services.
The security and vulnerability management segment is expected to hold the largest market size during the forecast period, owing to the increase in complicated as well as advanced threats and malware attacks.
Accretion of digital technologies and industrial systems, convergence of IT and OT systems, and exponential rise and sophistication of cyber-attacks drive the Threat intelligence market growth.

MARKET SEGMENTATION

By component, the market is segmented into solutions and services. Based on application, the market is fragmented into information security management, log management, risk management, identity & access management, and others. Based on the deployment, the market can be divided into on-premises and cloud-based. Based on enterprise size, the market is fragmented into large enterprise and small & medium enterprises (SMEs). Based on industry verticals, the market is segmented into healthcare, BFSI, IT & telecom, retail and e-commerce, and others.

From a geographical standpoint, the market is categorized into North America, Europe, Asia Pacific, Latin America, and the Middle East and Africa.

4.2.3.3 COMPETITORS

Asia Pacific countries are increasingly investing in threat intelligence projects. The region comprises emerging economies, such as Australia, South Korea, and Rest of Asia Pacific. The region is a mix of developing and developed countries with the maximum presence of SMEs. The growing attacks are increasing the vulnerability of critical data stored by organizations. These attacks are adversely impacting revenue; therefore, with respect to these statistics, enterprises and governments in APAC have started investing more and more in threat intelligence solutions.

The key players covered in the threat intelligence market include IBM (US), Cisco (US), Trend Micro (Japan), McAfee (US), Mimecast (UK), VMware (US), AT&T (US), Check Point (Israel), DXC Technology (US), Broadcom (US) and NSFOCUS (US). Other players include CrowdStrike (US), Juniper Networks (US), ThreatConnect (US), Fortinet (US), Anomali (US), Forcepoint (US), LookingGlass (US), LogRhythm (US), Recorded Future (US), Optiv (US), SecLytics (US), EclecticIQ (Netherlands), Cyware (US), Cymulate (US), CYFIRMA (Singapore), SOCRadar (US), and Keepnet Labs (UK).

4.2.3.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Accretion of digital technologies and industrial systems	• High procurement costs of threat intelligence solutions

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• R&D investments by governments and enterprises to develop robust threat intelligence solutions for the protection of critical infrastructure	• Lack of trained security analysts to analyse threat intelligence systems

4.2.4 EVENT EVOLUTION PREDICTION

4.2.4.1 MARKET SITUATION AND TRENDS

The Event Evolution Prediction tool provided by CERTH is focusing on crowd flow and crowd density prediction in public places with emphasis to uncover anomalies in the typical hourly/daily trends that might indicate unexpected upcoming events and potential threats to public safety due to overcrowding. Being a relatively novel and still under research product section, there are no specific data about the market interest. However, very useful information can be extracted by the closely related Crowd Analytics market, that can be identified as targeted market.

Crowd analytics market is focusing on the demand, growth prospects, restraints and trends of commercial solutions that provide in-depth analysis of crowd movement at large gathering locations, such as airports, stadiums and other public places. One of the major factors driving the adoption of crowd analytics software in retail is the shift towards a customer-centric approach. This allows businesses to make more informed decisions, improve work efficiency and profitability, and provide better customer experiences. Additionally, the growing number of tourists and the focus on developing smart cities is increasing the demand for crowd analytics solutions. These solutions help extract information about passenger traffic, length of stay, returning visitors, country of origin, mobility patterns, and people distribution.

Factor	Drivers	Barriers
Political	Rise in concerns about public safety and key infrastructure. Increase of ICT spending in developed nations.	
Economic	Increasing demand for Business Intelligence (BI) arrangements.	High initial upfront expenditure (cost of processing units and required sensors)
Social	Increase in the numbers of carriers and travellers. Increase in demand for better crowd distribution planning in smart cities.	

Factor	Drivers	Barriers
Technological	Development of IT appropriation	Lack of IT infrastructure (especially in developing nations)
Legal		Legal and ethical concerns in EU about GDPR protection.
Environmental	Concerns about carbon footprint and sustainability	

4.2.4.2 MARKET SIZE AND SEGMENTATION

The crowd analytics market is segmented based on solution type, deployment model, domain of application, end user and region.

Segment Type	Segment	Volume, Pattern
Solution type	Software	
	Service	
Deployment model	On-premise	Owns the major share of the market. Used mainly by large enterprises.
	Cloud	Owns a small share of the market but is expected to have a significant growth rate.
End users	Transportation	Owns the major share of the market and expected to grow by 2030
	Travel and tourism	Expected to exhibit the fastest growth rate. Expected to grow by 2030
	Consumers good and retail	Expected to grow by 2030
	Public safety	Expected to grow by 2030
Application domain	Mobility and Tracking	Accounted for the highest market revenue. Expected to growth following the overall trend of the market.
	Crowd Flow Management	Expected to growth following the overall trend of the market.
	Safety and Security	
	Others	
Region	North America	Owns the major share of the market. The presence of large key players in this district and innovation advantage support the global crowd analytics market in North America.
	Europe	Second greatest share of the market, anticipated to grow at a substantial rate. The rise in the security breach in physical security has enabled the key players to improve security and safety measures at public places
	Asia-Pacific	Projected to have the fast growth rate.
	Rest	

4.2.4.3 COMPETITORS

The top competitors in the crowd analytics market are: Nokia Corporation, Agt International, Nec Corporation, Walkbase, Spigit Inc., Sightcorp Bv., Wavestore, Savannah Simulations Ag, Crowdanalytix Inc., Securion Systems, Crowd Dynamics

4.2.4.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• The technical algorithms can be utilized for analytics in other domains related to spatiotemporal information such as traffic analytics. • The service depends solely on visual inputs (cameras) and does not require the use of other sensors/devices such as GPS.	• The implementation of the approach requires the use/installation of cameras to reads and public places. • The accuracy of the solution depends on the amount of data available (the number of cameras installed in the places of interest).

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• There is increasing focus and investment by governments and enterprises to develop public security solutions.	• Significant competition in a fast-evolving market that includes big competitors. • Data security and privacy concerns.

4.2.5 GEO-SPATIAL INTELLIGENCE

4.2.5.1 MARKET SITUATION AND TRENDS

Geospatial Intelligence in APPRAISE has the goal of reconnaissance and to obtain intelligence from the analysis of events, spatial information (geodata) and time.

Geospatial data analysis is a new market sector and is the process of collecting and analysing information about geographic objects and their relationships to the earth or other geographic objects. By using geographic information systems (GIS), data can be sorted, examined, analysed, results can be shown, conclusions can be clarified in a way that was not possible without GIS. The advantage is the combination of precise description and accurate location of events and objects on the earth's surface with the ability to integrate and display a variety of information about them.

Factor	Drivers	Barriers
Political	Governments and Organizations rising demand for big data analysis along with GIS	
Economic	Better decision making in combination with time and resource savings	High investment costs
Social		Social acceptance big data analysis
Technological	Newest state of the art GIS technology	Continuous innovation in the GIS market
Legal		Legal and ethical concerns in EU about GDPR protection.
Environmental		

4.2.5.2 MARKET SIZE AND SEGMENTATION

According to the marketsandmarkets [20] recent report, geospatial analytics market is projected to grow from USD 67.4 billion in 2022 to USD 119.9 billion by 2027, at a CAGR of 12.2% during the forecast period. With the use of GIS, earth observations, 3D scanning, satellite images, mapping, and many other geospatial technologies, geospatial analytics helps to collect, integrate, display, manipulate, and analyse geographical data. Governments and corporate organizations can now use geospatial data as a critical information source to make decisions about risk assessment and mitigation, disaster management, and urban development as well

4.2.5.3 COMPETITORS

The geospatial analytics vendors have implemented various types of organic and inorganic growth strategies, such as new product launches, product upgradations, partnerships and agreements, business expansions, and mergers and acquisitions to strengthen their offerings in the market. The major vendors in the global geospatial analytics market include Esri (US), Precisely (US), Caliper Corporation (US), Blue Marble Geographic (US), Google (US), eSpatial (Ireland), HexagonAB (Switzerland), TomTom (Netherlands), Trimble (US), Maxar Technologies (US), RMSI (India), Maplarge (US). General Electric (US), Bentley Systems (US), Fugro (Netherlands).

4.2.5.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Big data analysis	• High procurement costs of GIS solutions

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Enhanced agility, scalability and improved performance	• Lack of skilled analysts

4.2.6 RISK-BASED SURVEILLANCE ATTENTION

4.2.6.1 MARKET SITUATION AND TRENDS

This tool is responsible for creating an interface for end-users to be able to configure searches on the web and extract information through specific crawlers. The idea is also to add specific features that allow users to make the search more accurate (clustering of keywords related to the soft target to be monitored) in order to help the system and improve crawler results.

Innovation: adding the clustering of the main keywords linked to an event or the analysis of the sources to understand which may be the relevant for the selected use cases.

According to the Mordor Intelligence report [21], the data discovery and extraction market is expected to register a CAGR of 21% over the forecast period, 2022-2027. The data discovery market is anticipated to grow significantly over the future, owing to the increasing demand of businesses for visualization and explorative data analysis services. The data discovery market's primary growth drivers include the growing importance of data-driven decision-making, growing trends in self-service business intelligence (BI) tools, and insight generation from a growing number of multi-structured data sources. Data discovery market applications apply visual tools comprising geographical maps, heat maps, and pivot tables to make the process of finding patterns faster and more intuitive.

- Based on types, the data discovery software segment is anticipated to gain prominence in the data discovery market soon. Data discovery and visualization Software like Tableau, QlikView, and Tibco Spotfire are designed for data analysis and technically oriented business uses.
- According to Import.io Inc., web data is projected to grow faster due to both machine-based and human-generated data experiencing an overall growth rate of 10 times faster than conventional business data. With such significant potential, 89% of users believe big data will revolutionize business operations in the same way the internet did.
- Besides, the data discovery market will face challenges in security and privacy. Cloud-based solutions may pose security threats due to the extensive data collection that is stored by third-party entities. Apart from that, uncertain return on investment (RoI), complicated tools, and limited applications are other factors restraining the growth of the market.

Factor	Drivers	Barriers
Political		High political attention to avoid equip Public Authorities with mass-surveillance tools, or non-discriminated collection of information from the web
Economic	Increasing demand for data discovery and extraction tools	Recent worldwide crisis (COVID-19, Russia-Ukraine conflict, energy prices) has negative effects on public

Factor	Drivers	Barriers
	Tools easily deployed in other sectors, thus representing more exploitation opportunities	expenditures, thus less investments in technological tools
Social		Social acceptance of data collection and surveillance tools
Technological	Last advances in technology innovations (software & hardware) facilitate launch of cutting-edge innovative solutions	Increased and continuous competition of innovative solutions from highly specialized companies
Legal		Legal and ethical concerns in EU about GDPR protection.
Environmental		Concerns about carbon footprint and sustainability since data analytics tools require typically high processing high-power consumption

4.2.6.2 MARKET SIZE AND SEGMENTATION

Global data discovery market size reached USD 8.17 Billion in 2021 and is expected to register a revenue CAGR of 21% during the next years. Steady market revenue growth of the data discovery market can be attributed to increasing necessity to locate sensitive structured and unstructured data and discover new patterns and outliers to better understand any insights data from an organization can provide.

On the basis of component, the data discovery market has been segmented into solutions and services. Services segment is expected to register a rapid revenue growth rate over the forecast period. This can be attributed to increasing adoption of data discovery services globally. Employees, business partners, and clients have access to enterprise data, which is stored in a number of locations and storage systems. It is essential for any organization to identify and categorize data in order to secure and gain knowledge from the information. With the help of data detection, enterprises can recognize who has access to and where company data is located, understand which data is transmitted, how it is done, and over what channels. It can also be used to classify data manually or automatically, determine, categorize, and track sensitive data, execute risk management and compliance evaluation, display datasets and their applications, and utilize guidelines to manage and safeguard data in accordance with the circumstances, thereby reducing the likelihood of data migrations.

Solutions segment is expected to account a largest revenue share during the upcoming years. An organization's need for analytical solutions is supported by data discovery solutions. Companies need data discovery solutions in order for various types of business users to be able to make informed business decisions. These technologies can be used by business analysts, for instance, to spot crucial patterns and connections in data that could be used to improve a company's marketing or sales efforts. Data discovery solutions enable business users to explore and interact with an organization's data more easily while also providing enterprises with a comprehensive view of their information assets. Even non-technical users can access insightful data without needing to acquire data modelling and other new abilities.

4.2.6.3 COMPETITORS

The data discovery market is moderately competitive and consists of a few major players. In terms of market share, some of the players currently dominate the market. However, with the advancement in analytics. New players are increasing their market presence, thereby expanding their business footprint across the region. The vast expansion of capabilities in the big data analytics technology (owing to the availability of open-source tools) may also push the companies in the area to keep up with rivals and give away too much of the improved product performance, and the environment escalates costs and erodes industry profitability.

The data discovery vendors have implemented various types of organic as well as inorganic growth strategies, such as new product launches, product upgradations, partnerships and agreements, business expansions, and mergers and acquisitions to strengthen their offerings in the market. The major vendors in the global data discovery market include IBM (US), Microsoft (US), Oracle (US), Salesforce (US), SAS Institute (US), Google (US), AWS (US), Micro Focus (UK), MicroStrategy (US), Cloudera (US), PKWARE (US), Alteryx (US), Thales (France), Spirion (US), Egnyte (US), Netwrix (US), Varonis (US), Digital Guardian (US), Exonar (UK), Nightfall (US), Securiti (US), DataGrail (US), Dathena (Singapore), BigID (US), Explorium (US), 1touch.io (US), Congruity360 (US), and Concentric (US).

4.2.6.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Growing need to discover useful structured and unstructured data	• Lack of skilled professional workforce

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Increasing demand to integrate data in business processes to derive actionable insights	• Data security and privacy concerns

4.3 INTERNET CONTENT ANALYSIS TOOLS

4.3.1 DATA ACQUISITION AND PRE-PROCESSING FROM SURFACE AND DEEP WEB SOURCES

4.3.1.1 MARKET SITUATION AND TRENDS

Any information that can be legally collected from free, public sources is referred to as open-source intelligence (OSINT). In practice, this usually refers to data and material found online on the Internet, but in principle, any public information falls under the category of OSINT, such as books or reports in a public library, articles in a newspaper, or statements in a press release. Regarding the online aspect of OSINT, it includes information obtained mainly through social media monitoring, deep and dark web monitoring, Email hacks, Internet archives searching, Link analysis, etc.

In order to discover, extract, and acquire online material, Web crawlers are used, i.e., software programs that perform crawls and searches and automatically index website content and other information over the Internet. The market for global Web crawler software is predicted to grow significantly by 2030. According to ReportLinker [22], the global web scraper software market is expected to grow at a compound annual growth rate of over 3% by 2030, from USD 149.09 million in 2018 to USD 196.88 million in 2030. The market for online scraping software is expanding as a result of several important aspects, including development activity that is in accordance with demand and market conditions, market risks, assessments of new technologies, acquisitions, and the adoption of new trends. The need for web scraping software is also anticipated to rise as a result of an increase in R&D activity across various industries. Search Engine Crawlers (SECs), are web crawlers that find new web pages just like a user while surfing the internet through hyperlinks. When they retrieve a page, they save all the URLs it contains. The collected information is usually evaluated and stored via indexing so that it can be found quickly. Social media crawling is also another segment of OSINT, which is flourishing and it refers to the process of automatically extracting data from social media platforms such as Twitter, Facebook, and Instagram. With a total of over 6 billion active users [23] in the world's biggest social media platforms, there is an ever-growing market of social media crawling tools.

Factor	Drivers	Barriers
Political	• Keep up with potential changes to legislation laws and regulatory bodies	• Restricted access to the web for political reasons makes online data acquisition significantly more difficult, since the use of the tools must meet relevant regulations. Some countries have more specific Internet regulations, which broadly permit the use of such tools, but prohibit the distribution of certain knowledge.
Economic	• Growing demand for business intelligence • Maintaining data freshness	• Relatively consuming in terms of resources and time, due to the vast amount of time that new pages need in order to be indexed

Factor	Drivers	Barriers
		and due to the high percentage of broken links in the search engines
Social	• Gaining and maintaining the trust of the society	• Societies tend to show lack of trust to such tools, due to a general feeling that those tools can be used for questionable or ethically dubious reasons
Technological	• Keeping up with changes in information technology, life cycle and speed of technological obsolescence.	• Anti-crawler protection software is being developed and web crawlers have to overcome also this barrier • Web servers hosting the Web pages have different rules such as rate and resource limitations
Legal	• Comply with privacy and data protection legislation	• Different legislation among countries may have a negative effect to the data collection and/or storage • Terms of Services can affect the type of content collected
Environmental	• Comply with the changes in energy consumption limits due to the energy and environmental crisis	• Energy crisis that emerges in Europe might also affect services and databases

4.3.1.2 MARKET SIZE AND SEGMENTATION

OSINT market is a flourishing one and according to forecasts [24], it will continue growing the following several years. The market segment for general-purpose Web crawlers is anticipated to experience the greatest compound annual growth rate of 15.2% [25] during the next decade. General-Purpose Web Crawlers, Focused Web Crawlers, Incremental Web Crawlers, and Deep Web Crawlers are the four types of web crawlers that make up the global web crawler software market. As a result of the fact that these cutting-edge technologies can extract data from online forms, scrape essential website data, harvest corporate and personal email data, and more, the General-Purpose Web Crawler segment dominated the market in 2018 with a revenue share of over 30%. This tool can be used by organizations to increase the analysis of unstructured data, find trends in document collections, find pertinent information on competitor websites, and generate qualified leads. Social media crawling and web engine search market segments, also offer a continuously growing variety of specialized tools based on the targeted platforms.

OSINT, can attract various stakeholders from different sectors such as Industry, Public sector, individuals etc. For example, the information gained by OSINT could be invaluable to marketing teams to keep a pulse the market image through sentiment analysis. It also can provide knowledge about the customers' perceptions and how the companies are comparing against the competition. OSINT has also become an invaluable tool for the public sector. It has been adopted by national and

international security policies, supporting and helping public sector in different use cases including counter-terrorism, cybersecurity, disinformation etc.

In terms of geography growth, by 2027, Asia-Pacific countries will hold a 35% share of the market, according to projections [26]. Given the degree of technological advancement in the nations of this region, such as Japan or South Korea, this number makes sense. Given that the majority of major tech companies are based in the US and Canada, it makes sense that North America will account for 27% of the OSINT market. The Middle East and Africa will account for 11% of the market, Europe for 20%, and Latin America for 7%.

4.3.1.3 COMPETITORS

The Global Web Crawlers Market segment is flourishing and has been segmented into Cyber Security Organizations, Military & Defence Intelligence Agencies, Government Intelligence Agencies, Law Enforcement Agencies, Financial Services, Private Specialized Business, and others. Google LLC, Thales Group, Expert Systems S.p.A, Alfresco Software, Digital Clues, Maltego Technologies GmbH, Palantir Technologies, Recorded Future are some of the market's top competitors. Regarding the Social media crawling, there are many applications developed by the industry, which can extract data from the social media platforms. Some of the market's top competitors are Dripify, Octoparse, Apify, ScrapingBee. Regarding search engine crawling, most of the world's biggest companies offer their own solutions. Namely, some of the biggest competitors are Google LLC, Microsoft, Yahoo, Baidu, DuckDuckGo, Meta. Considering the high availability of solutions in the OSINT field, it is relatively easy for the customers to change providers, according to their needs, making the market volatile, thus providing the opportunity to interested parties to offer their solution and try to claim their share.

4.3.1.4 PARTNERS AND PROVIDERS

Both in terms of Social Media Crawling and the Web Search, the respective tools depend on the social media platform providers. As they gather the content through APIs, they need the respective API keys in order to be able to perform their tasks in both social media and search engines.

4.3.1.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Filtering capabilities-relevant content • Surface web, dark web & social media crawling capability • Unified User-friendly interface • Public interest • Time-efficient • Pseudonymisation of personal information	• Data validation (Fake news) • No mobile application

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Emerging technologies	• Anti-crawling software

	• Policies and legislation both in national and international level

4.3.2 MONITORING OF CRIMINAL INTENT THROUGH ONLINE TEXTUAL CONTENT ANALYSIS

4.3.2.1 MARKET SITUATION AND TRENDS

There are two main markets utilising textual analysis to gather context from raw textual data. The much larger of these is data analysis services including brand monitoring of companies or products, market research on demographics or users, and resulting applications such as recommendation systems and trend analysis. Textual analysis in these contexts is normally attempting to extract as much contextual information as possible to understand and explain phenomena such as how sentiment on product reviews is affecting product sales or how a political campaign is received. Open-Source Intelligence (OSINT) is also a sizable market for indicator extraction, applied specifically to intelligence gathering. Normally associated with police forces, OSINT is typically used to gather evidence of online criminal activity as evidence or indicators of crimes, with less resources required than physical evidence gathering.

Factor	Drivers	Barriers
Political	Online data as a continually growing market makes analysis of this data more of a priority for information gathering.	Fear of public perception of collateral collection or profiling, where analysis can be seen as invasive or in conflict with public privacy.
Economic	Performance of analysis models continues to improve, reducing the hardware cost of doing data analysis.	Policy such as GDPR requires data analysis to ethically collect, analyse and securely store data for only set periods and reasons, resulting in high costs for hiring domain experts as these issues get more complicated.
Social	Online communities continue to diversify and expand, resulting in a variety and scope of data that is very powerful if analysed appropriately.	Multitude of platforms, formats and scopes of online communities to analyse means analysis becomes a more and more fragmented field.
Technological	Improvements in open-source library space, shrinking of model sizes, and wide availability of analysis models results in lower requirements for deploying and maintaining tools.	Privacy concerns, fears of automated bots or other spam, and monetisation mean online platforms are becoming more difficult to access, shutting off APIs and restricting scraping so there is less data to analyse.
Legal	Frameworks such as the AI Act and AP4AI continue to raise awareness of how data analysis and Machine Learning is used, reducing fears of surveillance, improving citizen trust, and allowing analysis to be	Strengthened legal requirements such GDPR and the AI Act mean analysis, especially when Machine Learning based, must abide by higher and higher requirements.

Factor	Drivers	Barriers
	performed in a better-defined legal space.	
Environmental	Reduced model sizes significantly reduce environmental impact of machines that analysis is run on.	Improved efficiency of models used in deployment is often at the expense of large pre-trained models on high performance machines.

4.3.2.2 MARKET SIZE AND SEGMENTATION

The majority of the data analysis market is private sector companies leveraging data analysis to gather feedback, test products, and improve their business. As online data availability continues to expand tools continue to improve, this market segment will heavily expand as companies expand their engagement with their users online.

The next largest segment is analysis by states and governments on citizen feedback, polls, surveys and other data that can be leveraged further. Due to governments having access to large amounts of data in various different formats, further analysis of this data allows insights to be collected from multiple formats, combined across data sources, and presented to inform policy in a wide variety of contexts. This market segment is expected to grow as accessibility to data analysis techniques increases, allowing governments to leverage their data for further insights.

The OSINT market is a relatively small subset of the data analysis market, as this is analysis applied to data in the intelligence domain specifically. As both the variety of OSINT data increases from additional platforms, online communities, and collection techniques, the difficulty of obtaining data for this purpose is increasing with APIs being closed, scraping being prevented, and the web becoming more hostile to automation. Both factors as well as market saturation of tools will result in this segment staying roughly the same size.

4.3.2.3 COMPETITORS

Generalised data analysis platforms such as IBM Buisiness Analytics[1] and AWS analytics[2] serve as general use analysis, typically paired with cloud services. While these analytics are powerful and wide-reaching toolkits, they are typically expensive and not specialised for specific needs of different use cases, requiring domain experts.

More specific applications of data analytics include Brandwatch[3] for online brand awareness and SurveyMonkey[4] for analysing survey feedback in more detail. These specialised data analysis as a service applications normally allow for analysis on a smaller, manageable scale for specific use cases.

Neither specialised nor generalised analysis services like these compete with analysis performed in APPRAISE, as the ease of use and online service nature of these providers makes them ill-suited to real-time early warning, sensitive data storage, and modification to specific APPRAISE use cases, though the tools uses for analysis can be similar.

[1] https://www.ibm.com/uk-en/analytics/business-analytics
[2] https://aws.amazon.com/free/analytics/
[3] https://www.brandwatch.com/
[4] https://www.surveymonkey.co.uk

More direct competitors are in the OSINT space, as these tools consider the sensitive data storage through being police investigation focused. Large analysis services such as LongArm[5] and Palantir[6] provide investigation focused analysis tools but are still expensive for low resource investigations.

4.3.2.4 PARTNERS AND PROVIDERS

Data analysis is dependent on the collection and aggregation of large amounts of online data. This makes data analysis of criminal intent against soft targets through online textual content analysis on the web and social media data collection by CERTH in APPRAISE.

4.3.2.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Extraction steps can be swapped, disabled or added for different contexts • Lower resource analysis as on individual pieces of content rather than large datasets • Leverages insights from data automatically for user prioritisation	• Support for less common languages is weak for certain extraction types • High memory requirements when loading multiple models

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Growing market of tools and models as methods are made more effective • Growing amount of online content to analyse	• Growing privacy and data storage constraints • Reduced access to online data on certain platforms

4.3.3 DETECTION OF TERRORIST ACTIVITY INDICATIONS IN MULTIMEDIA CONTENT

4.3.3.1 MARKET SITUATION AND TRENDS

The analysis of multimedia data in this context refers to the analysis of audio and video/image data, captured through targeted search from the internet. The analysis of text, as a direct functionality or at posterior stage, is considered in the section 4.3.1.

The specific analytics module that we will refer to are:

- Audio modality: transcription of audio to text, with possible posterior text search for keywords that are related to public security.

[5] https://www.digitalmarketplace.service.gov.uk/g-cloud/services/210748352904117
[6] https://www.palantir.com/uk/

- Video/image modality – general: recognition of text in the captured scene, as well as scene geo-localisation.
- Video/image modality – security related: detection of security events captured by static (CCTV) or mobile cameras (i.e., by event participants); examples of events of interest may include panic and fight.

While the first two modules refer to functionalities of general application, the last one is specific to perception and management of public security, and its final application to marked may thus be more limited by the end user group or domain.

Therefore, the key market for this tool would include mainly LEAs and other (private) security companies. According to business reports, the Global Security and Surveillance market is estimated to be valued at US$ 17.68 Bn in 2022 and is projected to increase at a CAGR of 4.8% in the forecast period from 2022 to 2032.

Growing safety and security concern, gathering of evidence of some irregular activities and to maintain its record are responsible for growth in Security and Surveillance used in various sectors.

According to another report, “the developing critical infrastructure which includes commercial sectors like financial services, government offices, business zones, institutions, emergency services, IT services, transportation are needed high level of security to prevent activities or accident before they occur. Almost every of these sectors install Security and Surveillance Equipment like CCTV camera’s, audio equipment to record the video or audio evidence of the incident which had been happened at those respective places. Similarly, most of the industry is having risk of occurring of hazardous incident like fire catching, accident of any labour or failure of any equipment. For this not to be happened, almost every industry and factory owner install security surveillance equipment for industry safety and relentlessly monitoring of the plant site. Nowadays, the most chances of crime like theft, robbery and any violence are to government buildings and residential buildings. To fight theft, violence, and vandalism, efficiently, buildings owners are installing new-generation CCTV cameras, by which they can detect and interpret suspicious incidents by themselves. This Security and Surveillance Equipment systems also have the capability to cooperate with other systems, such as alarm systems. All of these factors are driving the market for Security and Surveillance Equipment Market”.

Factor	Drivers	Barriers
Political	Regulation	Disparities among several countries
Economic	Prevention of crimes and economic losses	Investment in technological solutions
Social	Confidence in technology and user acceptance	Privacy and security concerns
Technological	Mature technologies	Integration with legacy systems
Legal	Regulation	Privacy concerns
Environmental	Disaster prevention	

4.3.3.2 MARKET SIZE AND SEGMENTATION

As aforementioned, the key market for this tool would include mainly LEAs and other (private) security companies. According to business reports, the Global Security and Surveillance market is estimated to be valued at US$ 17.68 Bn in 2022 and is projected to increase at a CAGR of 4.8% in the forecast period from 2022 to 2032.

According to the Global Security Surveillance Market (2022-2027) research report [27], we can identify the following segments:

Security Surveillance Market Segmentation by Type:

- Security Cameras
- DVR and NVR (Digital and Network Video Recorder)

Security Surveillance Market Segmentation by Application:

- Residential Use
- Commercial Use
- Public and Government Infrastructure

Security Surveillance Market Geographic Segmentation:

- North America (USA, Canada, Mexico)
- Europe (Germany, UK, France, Russia, Italy, Rest of Europe)
- Asia-Pacific (China, Japan, South Korea, India, Southeast Asia, Rest of Asia-Pacific)
- South America (Brazil, Argentina, Columbia, Rest of South America)
- The Middle East and Africa (Saudi Arabia, UAE, Egypt, Nigeria, South Africa, Rest of MEA)

The key priority market for the APPRAISE tool would be LEAs (public and government infrastructure) in the EU Member States, starting with those involved in the project.

4.3.3.3 COMPETITORS

A list of BEST KEY PLAYERS Listed in the Security Surveillance Market Report are:

- Hikvision
- Dahua Technology
- Axis Communications AB
- Panasonic
- Honeywell Security
- Hanwha
- Tyco
- Bosch Security Systems
- Pelco
- Samsung
- Uniview
- Flir Systems, Inc.

Moreover, there are several commercial Speech-to-Text solutions, such as:

- Google Cloud Speech-to-Text
- Dragon Speech Recognition Software
- Microsoft Bing Speech API
- Amazon Transcribe

- IBM Watson Speech to Text
- NICE CXone
- Krisp
- Talkdesk
- Invoca

The APPRAISE module would, however, provide an integrated solution for multimedia content analysis, which would be specifically targeted to the LEAs needs (e.g., detection of terrorist activities).

4.3.3.4 PARTNERS AND PROVIDERS

- The component is not dependent on a provider (e.g., hardware component for the drone, specific microphone device), the software developed is hardware agnostic, but can be customised to the specific needs and requirements of the end users.
- Potential partners and partnerships would include collaboration with device manufacturers, so the SW module is optimised for a specific HW. Such a joint endeavour would produce a final product that would integrate the intelligent algorithms in the actual security device (camera/microphone).

4.3.3.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Specific software development tailored to the concrete client needs	• Current tools not developed for this domain, need to be adapted.

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Market growth and need for technological solutions	• Difficulty to test solutions with real operational data

4.3.4 IDENTIFICATION OF RELEVANT PEOPLE AND CRIMINAL GROUPS FROM ONLINE CONTENTS

4.3.4.1 MARKET SITUATION AND TRENDS

The tool generates an automatic characterization of social media Users analysing recent User posts and considering also the contents posted by its connected Users. This characterization can be then used by LEAs to determine if a User is a potential threat or not.

Being specifically built to be used on social medias, it is reasonable to believe that the market of our tool aligns well with the general social media market.

Factor	Drivers	Barriers
Political	Anti-terrorism	Privacy, regulations, social media data sharing policies
Economic	Growing social media usage and linked commercial applications	Privacy, regulations, social media data sharing policies
Social	Moderation of online content in social medias	Potential privacy breach, Potential biases introduced by the algorithm
Technological	Developing Deep learning application to graph	Poor classification accuracy due to the absence of wide reference datasets
Legal	New policies introducing the need to validate contents posted on social media	Privacy, regulations, social media data sharing policies
Environmental	New policies to reduce greenhouse gases emission	Deep learning is not environmentally friendly due to the computational resources needed, which are higher with respect to other algorithms

4.3.4.2 MARKET SIZE AND SEGMENTATION

The social media analytics market was valued at USD 7.26 billion in 2020 and is expected to reach USD 25.96 billion by 2026, at a CAGR of 23.3% over the forecast period 2021 - 2026 [28]. Social media analytics is widely considered to be a significant business and marketing tool in the present-day business scenario. In order to gain actionable insights on consumer perceptions and improve their services and products portfolio, businesses across the world are using social media analytics.

The rise of mobile phones and tablets with access to the internet, coupled with ever growing user volume on social media platforms, is boosting the growth of the social media analytics market over the forecast period. Incremental technological advancements may pave the way for several growth opportunities by making social analytics tools more accessible to the small/medium scale organizations all over the world. The demand for social analytics tools has been bolstered by the increased emphasis on consumer feedback, as they exhibit greater bargaining power in the market. Currently, the consumer is accessible through social media platforms further reinforcing the need for social media analytics tools for enterprises globally. According to Facebook, it had 1,56 million active users daily, as of the first quarter of 2019. In fact, Twitter stated that 500 million Tweets are sent each day and 9% more people are using Twitter every day, reinstating the growing penetration of social media networks at a global level [29].

4.3.4.3 COMPETITORS

Key commercial players in the field of social media User characterization and classifications are:

- Facebook (FB and Instagram)
- Twitter
- Google (Youtube, Youtube Music)
- TikTok

The core of these products is a proficient content recommendation system that is based on User characterization. On top of that these companies have access to a massive volume data, available for them on their platforms, to train their algorithms. Therefore, one would assume the most advanced algorithm for graph user embedding are developed by these companies.

4.3.4.4 PARTNERS AND PROVIDERS

The tool is dependent on the social media (Twitter) API to retrieve relevant data.

4.3.4.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• The tool has been developed specifically for APPRAISE therefore it is tailored on the LEAs requirements	• Data availability, both for training and production • Restrictions introduces by social media APIs • Support is limited to Twitter, which is the sole social media allowing to programmatically fetch data through APIs. • Classification accuracy to be validated

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Social media market is huge and rising, so it provides many opportunities to employ such tools	• Restrictions related to the API usage policy.

4.3.5 CONTEXT-BASED RISK ASSESSMENT OF SOFT TARGETS

4.3.5.1 MARKET SITUATION AND TRENDS

The risk assessment has the task of collecting information input from tools and services, aggregating them by applying context-based rules coming from end-users' domain requirements and generating a risk value associated with the OSINT data, e.g. coming from social media.

Innovation: assessment of the level of risk based on real analyses made by the LEAs and based on operational parameters and agents' experience and risk evaluation judgements on social media post.

According to MarketsandMarkets report, globally, the adoption of risk analytics software solutions has shown a good pace. These solutions are critical to generating actionable insights, thus enabling C-level executives to make informed decisions. Software solutions, including Extract, Transform, and Load (ETL) tools; risk calculation engines; scorecard and visualization tools; dashboard analytics and risk reporting tools; and GRC software, are offered to tackle risk management challenges. The services offered in the market are professional services and managed services. The services segment is projected to grow faster during the forecast period.

The global risk analytics was valued at USD 26.81 billion in 2020 and is expected to reach a value of USD 52.33 billion by 2026, while registering a CAGR of approximately 14% over the forecast period, 2021 - 2026 [30]. Risk analytics solutions help organizations deal and protect against operational risks, which can arise due to internal factors, such as human errors, failures of systems (which can be related to software, hardware, network, etc.), and fraud cybercrime.

Factor	Drivers	Barriers
Political	N/A	
Economic	Increasing demand for risk assessment tools Tools easily deployed in other sectors (including cybersecurity), thus representing more exploitation opportunities	Recent worldwide crisis (COVID-19, Russia-Ukraine conflict, energy prices) has negative effects on public expenditures, thus less investments in technological tools
Social		Social acceptance of risk assessment tools based on collection and analysis of personal data
Technological	Last advances in technology innovations (software & hardware) facilitate launch of cutting-edge innovative solutions	Increased and continuous competition of innovative solutions from highly specialized companies
Legal		Legal and ethical concerns in EU about GDPR protection.
Environmental		Concerns about carbon footprint and sustainability since data analytics tools require typically high processing high-power consumption

4.3.5.2 MARKET SIZE AND SEGMENTATION

In line with above forecasts, the global risk analytics market size to grow from USD 39.3 billion in 2022 to USD 70.5 billion by 2027, at a Compound Annual Growth Rate (CAGR) of 12.4% during the next five years [31]. Various factors such as rising government compliance with stringent industry regulation, growing incidences of data thefts and security breaches and increasing complexities across business processes, are expected to drive the adoption of risk analytics solutions and services.
Risk analytics solutions help organizations to deal and protect against operational risks, which can arise owing to internal factors, such as human errors, failures of systems (which can be related to software, hardware, network, etc.), and frauds, including cybercrime. Vendors are offering this software through on-premise and cloud deployment for end-user industries, such as BFSI, Healthcare, IT, and Telecom, which are considered in this study.

4.3.5.3 COMPETITORS

The risk analytics market is relatively a consolidated market as the major vendors account for a significant share of the market, especially in the enterprise-level adoption. Additionally, the large companies dominate this market owing to their ability to offer innovative and high-quality services to end-users on a different scale and with customization that suits their specific needs.
The Risk analytics vendors have implemented various types of organic and inorganic growth strategies, such as new product launches, product upgradations, partnerships and agreements, business expansions, and mergers and acquisitions to strengthen their offerings in the market. The major vendors in the global Risk Analytics market include IBM (US), SAP (Germany), SAS (US), Oracle (US), FIS (US), Moody's Analytics (US), Verisk Analytics (US), Alteryx (US), AxiomSL (US), Gurucul (US), Provenir (US), BRIDGEi2i (India), Recorded Future (US), AcadiaSoft (US), Qlik (US), DataFactZ (US), CubeLogic Limited (UK), Risk Edge Solutions (India), Equarius Risk Analytics (US), Quantifi (US), Actify Data Labs (India), Amlgo Labs (India), Zesty.ai (US), Artivatic (India), Artivatic (US), RiskVille (Ireland), Quantexa (UK), Spin Analytics (UK), Kyvos Insights (US), Imply (US).

4.3.5.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Increasing complexities across business processes	• Intricate nature of regulatory compliance

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Rising innovations in the FinTech industry	• Integration of data from data silos

4.4 PUBLIC-PRIVATE INTEROPERABILITY AND COLLABORATION SERVICES

4.4.1 CONTEXT INFORMATION INTEGRATION AND HARMONIZATION

4.4.1.1 MARKET SITUATION AND TRENDS

The information integration and harmonization tool aims at transforming data (coming from the sub layers of the architecture) into outputs for the visualization in the DITHO app. The main step regards the normalisation and propagation of the data. In a scenario where different systems interact, interoperability is essential. Interoperability in terms of Connectivity (to manage different protocols – output of the tools) and Normalisation (to merge different data formats).

The Context Information Integration and Harmonization tools can be classified under the market category of Enterprise Data Management tools. According to ResearchandMarkets [32] latest report, the global enterprise data management market size is expected to reach USD 265.68 billion by 2030 and grow at a CAGR of 14.0% from 2022 to 2030. The growing need for on-time data delivery and digitalization are the major driving factors for this growth. Enterprise Data Management (EDM) includes various features such as flexibility to choose multiple deployment modes, robust quality controls, and accessible distribution functionalities. It addresses the data availability concerns by procuring data from multiple locations and sources, and storing is in a single common platform. These benefits help businesses and enterprises organize and manage their data better and enable efficient data-based decision making.

Factor	Drivers	Barriers
Political		
Economic	Increasing demand for data management tools as available data is becoming more a more massive	Recent worldwide crisis (COVID-19, Russia-Ukraine conflict, energy prices) has negative effects on public expenditures, thus less investments in technological tools
Social		Social acceptance how data management tools handle collection and processing of personal data
Technological	Last advances in technology innovations (software & hardware) facilitate launch of cutting-edge innovative solutions	Increased and continuous competition of innovative solutions from highly specialized companies
Legal		Legal and ethical concerns in EU about GDPR protection.
Environmental		Concerns about carbon footprint and sustainability since data analytics tools require typically high processing high-power consumption

4.4.1.2 MARKET SIZE AND SEGMENTATION

Due to the rising demand for regularly handling massive data generated in companies, enterprise data management solutions are gaining traction. Organizations generate different types of data, including financial information, photos, graphics, videos, inventory numbers, mobile data, and social media data, from various organizational assets. The amount of data collected and processed by organizations that may be used to their advantage is increasing, putting data management high on their agendas. Furthermore, several organizations from many industries have their offices all over the world and their data varies depending on the location of the firms, posing a difficulty for data procurement. As a result, EDM solutions facilitate single-source reporting and multi-user functionality, providing clients with consistent data in all locations.

Enterprise data management solutions streamline business operations and also derive necessary conclusions from data. It also formulates a strategy for business operations ensuring transparency in the overall enterprise system. They also smoothen the data flow and reduce cycle time for various tasks. This brings about efficiency and effectiveness in managing enterprises. by acting as a master data management platform, enterprise data management provides customer data which includes onboarding of new client data to integrate into the internal systems of organizations. Moreover, enterprise data management addresses circumstances where users within an enterprise independently model, manage, store, and source data.

Market segmentation and features of Enterprise Data Management tools:

- The professional services segment held the largest market share of over 68.0% in 2021. The segment growth can be attributed to the increasing automation of professional services due to big data analytics and the growing demand for improved mobility among service consultants.
- The large enterprise segment accounted for a revenue share of over 67.0% in 2021. The segment growth can be attributed to the rising demand for robust monitoring solutions and automation capabilities for resource allocation and strategic decision-making across large organizations.
- The cloud segment held a revenue share of over 52.0% in 2021. The segment growth can be attributed to rapid adoption of cloud-based solutions by organizations as they eliminate the need for periodic manual upgrades and allow users to access data without any hassles irrespective of their location.
- The retail and consumer goods segment accounted for a market share of 11.4% in 2021. Companies operating in the retail and consumer goods industries have to fulfil customer expectations and keep the customers aware and update about the latest offerings. The retail industry is focusing on offering personalized products and services which can be conveyed to customers with the help of efficient data management solutions.
- The services segment is anticipated to register considerable growth at a CAGR of 15.7% over the forecast period. It helps businesses in reducing operating expenses, enhancing operational efficiency, and focusing on their core competencies. These factors will create the lucrative opportunities for the enterprise data management services over the forecast period.
- The Asia Pacific regional market is expected to reach USD 108.9 billion by 2030. The growing popularity of cloud computing and rising need to improve operational efficiency in large

enterprises and SMEs are expected to boost the demand for enterprise data management in the region over the forecast period.

4.4.1.3 COMPETITORS

The dominant players operating in the market include International Business Corporation; Oracle Corporation; SAP SE.; Cloudera, Inc.; Amazon Web Services (AWS); and Broadcom (Symantec); among others. Market players have been investing significant resources in R&D activities to support growth and enhance their internal business operations.

The companies can be seen engaging in mergers & acquisitions and partnerships to further upgrade their products and gain a competitive advantage in the market. They are effectively working on new product development, and enhancement of existing products to acquire new customers and capture more market shares. For instance, in April 2021, IBM Corporation launched a storage system for data management across hybrid clouds. The storage system is expected to improve data management across hybrid cloud environments, thereby improving data availability and flexibility. Some prominent players in the global enterprise data management market include:

- International Business Corporation
- Oracle Corporation
- SAP SE
- Cloudera, Inc.
- Amazon Web Services, Inc
- Teradata
- MindTree Ltd.
- Broadcom (Symantec)
- Informatica
- Micro Focus

4.4.1.4 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Increasing Requirement for Data Management System • Growing Emphasis on Regulatory Compliance	• Issues with Data Address and Validation

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Rising Adoption of Data Management Tools	• Security and Privacy Concerns

• Rapid Technological Advancements in Master Data Management Technology	

4.4.2 TOOLS FOR COMMUNICATION WITH THE CROWD

INOV as a research institute does not intend to explore commercially the crowdsensing application that is currently being developed in the scope of the APPRAISE project. INOV is mainly interested in exploring and applying state of the art technologies and to contribute to solutions that can help monitoring and securing soft targets with the main focus on implementing successfully the APPRAISE pilots. Nevertheless, INOV is fully available to give technical support within its area of expertise (mainly on implementing machine learning algorithms and techniques) to any partner that intends to reach the market and explore commercially their solution.

4.4.3 AR TOOLS FOR ON-SITE SITUATIONAL AWARENESS AND COLLABORATIVE TRAINING

4.4.3.1 MARKET SITUATION AND TRENDS

The augmented reality (AR) technological tools supplied by Holo-Light can be leveraged to aid in situational awareness and multi-user collaborative training. The software component generated by Holo-Light is the development kit ISAR (Interactive Streaming for Augmented Reality). ISAR provides a remote rendering capability which empowers high-quality AR services through streaming of AR applications and visualization of high-polygon content. Remote rendering with ISAR bolsters AR experiences by offloading the computationally demanding requirements from the end-user device and, by extension, allows a variety of higher-quality performance integrations with other application infrastructures. AR technologies have extensive use in many market sectors, which include, e.g., healthcare, education, and in industrial settings. Among the many core exploitable features of these technologies is the ability to provide infrastructure for efficient and robust delivery of information for a variety of users. This allows a diversity of use cases, such as collaborative training as well as the ability to access relevant intelligence at opportune or necessary critical moments. The usage of AR in such a capacity is growing across many sectors, such as e.g., the industrial sector [33] , which is further indicated by the amount of current and predicted spending and market prevalence on such technologies. Indeed, in a recent European Union strategic paper [34], an increase was reported in the European Union 2021 market size by 26% from 2020 and a compound annual growth rate was estimated to be 37% by 2026[Erreur ! Signet non défini.]. This expansion of interest and subsequent use has therefore seen considerable growth in recent years and appears to be steady in those to come. Providing high-quality information in the form of virtual content at convenient times is a marketable attribute for many of the aforementioned sectors where such measures can directly enhance performance metrics and output.

Factor	Drivers	Barriers
Political	Remaining competitive with global advances across industrial,	Potential to seem superfluous for public spending directives given AR

Factor	Drivers	Barriers
	consumer, and security sectors for AR streaming technologies.	could be viewed as being more applicable to consumer recreation.
Economic	Remote training and information delivery assists workers in making processes and workflows more time and effort efficient. Shared information optimizes speed of action, which reduces the number of resources spent.	Requires training on how to use the AR devices and software, thus some period of learning, and requires some infrastructure to implement it. Effort in changing existing work processes which people are accustomed to.
Social	Making training and information transfer easy between participants, AR visualizations and interactions facilitate better understanding of concepts and communication in real time. Workers can easily have needed information.	Worker groups/individuals might have prior beliefs that AR usage is either 1) not advanced enough to meet their demands or 2) too gamified to be of appropriate use in their working environments. Virtual collaboration removes the "in-person" atmosphere.
Technological	Software and hardware advancements in producing quality virtual content; specifically, remote rendering and streaming of content bypasses current AR device processing limitations.	Only few AR devices on the market which can provide suitable holographic visualizations for working settings. Such hardware is typically expensive and lacks high processing power on its own.
Legal	The usage, storage, and transfer of confidential, sensitive, and/or proprietary information is a necessary legal consideration. Encryption measures during AR information transfer significantly reduces the risk of sensitive information being hacked and ensures visualizations are accessible only by unauthorized users.	AR devices make use of cameras to map user hand movements for interaction with virtual content. In this manner, the presence of a camera may inadvertently lead people to believe that camera data is stored, and retained, which may lead to legal problems.
Environmental	AR remote collaborative training and information transfer events reduce the environmental demands that on-premises counterparts would require. E.g., transport to specific areas using modern transit methods is reduced; photographs need not be printed and distributed e.g., to law enforcement professionals at a situational event.	AR devices and corresponding remote rendering/streaming devices have energetic costs associated to them (i.e., one must run these devices) which presents with an environmental impact.

4.4.3.2 MARKET SIZE AND SEGMENTATION

The marketing segments for AR technologies, as mentioned previously, are rather diverse. Segments can range from public to private sectors and constitute multiple fields such as education, healthcare, retail, military/defence, and industrial players[7]. Engineering customers, of various types, can profit tremendously from incorporating AR technologies, particularly given the ability to visualize and manipulate three-dimensional holographic representations of specific machinery or job-content. Beyond engineers, a variety of other customers are able to profit as well, specifically those who utilize collaborative communication and information sharing, such as e.g., security and defence professionals. These examples serve to highlight the range of applicable market targets for AR technologies. With respect to AR streaming, such as ISAR mentioned above, the same segments can profit tremendously from the enhancement of AR environments with remote rendering. Stakeholders consist, for example, of members of the media who report and follow augmented and virtual reality advancements. AR technologies have been reported to be in a maturing phase [34], indicating that they are well established in the market and are progressing steadily forward. As mentioned above, a reported increase in the 2021 European market size by 26% from 2020 was found with predictions of further compound annual growth of 37% by 2026 [34] . In 2021, this market size was estimated at 9.6 billion Euros[Erreur ! Signet non défini.].

4.4.3.3 COMPETITORS

Augmented reality technologies are being explored by a considerable variety of market competitors. Some of these competitors in the field that actively engage with AR developments include technology companies such as, e.g., in nominal order:

- Meta Platforms, Inc.
- Google LLC
- Apple Inc
- Microsoft Corporation
- NVIDIA Corporation.
- Magic Leap, Inc.

The strengths of these companies are variable but often present in their global reach, infrastructure, and scope of deployable assets. Prominently, current market leaders dominate in the production of AR end-user devices, such as e.g., the Microsoft HoloLens[7], which provide some of best to-date hardware devices which provide optimal infrastructure to build AR solutions around. Beyond hardware, streaming technologies for augmented reality are an additional focus of market competitors. To highlight a few, NVIDIA Corporation provides AR streaming measures in the form of their CloudXR[8] solution and Microsoft Corporation offers Azure Remote Rendering[9].

4.4.3.4 PARTNERS AND PROVIDERS

ISAR-mediated remote rendering and streaming is accomplished on a personal computer or virtual machine, which is supplied by Holo-Light. However, the end-user device which receives the streaming flow and permits the user to visualize holographic information/content is the HoloLens which is

[7] Microsoft HoloLens | Mixed Reality Technology for Business
[8] VR, AR, and XR Streaming Solutions for Pro Viz | NVIDIA
[9] Azure Remote Rendering | Microsoft Azure

produced by the Microsoft Corporation[7]. An additional piece of hardware used in the APPRAISE project will be an extended reality input device Glock, created by MXR Tactics GmbH[10], which serves as an imitation model of a firearm. For the purposes of applicability in APPRAISE, integrations with the other consortium partners and their relevant components will also occur.

4.4.3.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Remote rendering and streaming of virtual content allow superior performance metrics, measurable in speed and hologram quality. • Usage presents with a high degree of device agnosticism, i.e., freedom of use across many device types. • A robust range of use cases are possible with AR visualizations and can be done collaboratively with multiple users.	• AR hardware end-user devices may not continuously be ergonomically or practically useful in certain situations. • AR information delivery requires a suitable network (e.g., Wifi) which may not always be available.

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Innovations in AR technologies are growing steadily and serve to enhance the entire business-field and exploitable possibilities. • Stronger desire in recent years for remote interaction, both professionally and in personal settings. • Consistent exponential growth in publicly available information necessitates methods of dissemination and visualization in a manner which allows ease of use and understanding (e.g., holographic visualizations assist here).	• Public opinion/belief that AR is mostly for recreation (e.g., too gamified). • Existing traditional processes (e.g., radio communication, verbal descriptions) may be engrained in a particular environment and users may not be open to adjusting to new technology.

[10] MXR Tactics - The future of AI-Based XR Trainings (mxr-tactics.com)

4.4.4 DISTRIBUTED COLLABORATIVE IMPROVEMENT OF SITUATIONAL AWARENESS TOOLS

INOV as a research institute does not intend to explore commercially the federated learning framework that is currently being developed in the scope of the APPRAISE project. INOV is mainly interested in exploring and applying state of the art technologies and to contribute to solutions that can help monitoring and securing soft targets with the main focus on implementing successfully the APPRAISE pilots. Nevertheless, INOV is fully available to give technical support within its area of expertise (mainly on implementing machine learning algorithms and techniques) to any partner that intends to reach the market and explore commercially their solution.

4.5 VISUALISATION AND DSS SERVICES, INCLUDING CYBER-SECURE CONTEXT INFORMATION AND INTELLIGENCE MANAGEMENT AND SHARING

This section presents the market analysis for the 3 indissociable tools provided by CS Group, namely:

- Intelligent Digital Twin-based Hypervision and Operation Management System (DITHO) (CS)
- AI augmented decision support (CS)
- Cyber-secure context information and intelligence management and sharing (CS)

The DITHO, in conjunction with the two complementary modules mentioned above, is based on CS Group's flagship product Crimson, it will enable the multi-dimensional situational awareness and operation management, by using a digital replica of the site to protect.

Originally, Crimson is a collaborative software solution designed for conducting operations, protecting sites, populations, and critical infrastructures, as well as for planning and managing crisis operations. The Crimson software solution facilitates the sharing of information, coordination and decision support by offering a clear, synthetic and global perspective on the situation. Throughout APPRAISE new capabilities facilitating the integration of the existing product with other components, along with interoperability with the mobile systems and connections to the C2. A module enabling the optimization of the response plans, aiming to advise and assist the user will be developed. More specifically, the AI augmented decision support will define the public spaces to be monitored and as a second step, develop and evaluate strategies to improve their security and resilience. Finally, in order for all the information to be shared in real time and across multiple users, from different organisations (public and/or private) and different countries in a secure way a cyber-secure context information and intelligence management and sharing module will be developed.

4.5.1.1 MARKET SITUATION AND TRENDS

The growing number of criminal activities and terrorist attacks, combined with the increasing need to protect cities, soft targets, critical infrastructures or sites have led to the growth of the respective markets targeted by the DITHO.

Market	Target	Market trends
Physical site security	Defence, industry and public or private security actors	The physical site security market size was valued at $104.6 billion in 2020 and is projected to reach $192.2 billion by 2030.

Market	Target	Market trends
		The CAGR is therefore of 6,5% for the period 2021-2030 [35].
Incident and emergency management	Civil security and firefighters	The anticipated CAGR of the incident and emergency management market is evaluated at 6,7% from 2021-2026. The growth from $124.0 billion to $171.8 billion by 2026 is due to the increasing criminal activities and terrorist attacks [36]
Public security and safety market	Public safety and defence actors	The anticipated CAGR of the public security and safety market is evaluated at 10,3% from 2022-2027, bringing it from $433.6 billion in 2022 to $707.2 billion by 2027.

The DITHO along with the associated modules is targeting the Public Safety and Security market. The tool can be used by both public or private security agents to efficiently prepare, organise and optimise the interventions during terrorist attacks. The table below provides a PESTEL analysis of the various Drivers and barriers identified for the DITHO.

Factor	Drivers	Barriers
Political	European strategy (cf. European Commission Drone Strategy) Organization of major events (e.g. Olympic games)	Applicable regulations Protocols and procedures when it comes to sharing information between public and private security actors as well as cross-border.
Economic	Single efficient solution compatible with legacy systems, enabling a single investment to optimise interventions.	Lack of budget to invest in new technologies.
Social	Better soft target protection and safety.	Mistrust with regards to AI and advanced technologies involving personal data use.
Technological		Reluctance to change practices Technological complexity Lack of visibility of the added value in comparison with existing solutions.
Legal		There might be specific local legal, regulatory or ethical and privacy regulations requiring additional measures

Factor	Drivers	Barriers
Environmental		Concerns about carbon footprint and sustainability

4.5.1.2 MARKET SIZE AND SEGMENTATION

The APPRAISE DITHO module, based on the existing CS GROUP product Crimson, will build on the existing functionalities by adding new ones specifically answering APPRAISE needs. This will create new market opportunities and will further enhance Crimson functionalities. Based on the targeted market, there are different market segments

Market	Segments
Physical site security (Pattern: growing)	- Component: System, Services - System type: Physical Access System, Video Surveillance System, Perimeter Intrusion and Detection, Physical Security Information Management, Others - Service type: (Access Control as a Service, Video Surveillance as a Service, Remote Monitoring Services, Security Systems Integration Services, Others - Enterprise size: Large enterprises, SMEs - Industry vertical: BFSI, Government, Retail, Transportation, Residential, IT, Telecom.
Incident and emergency management (Pattern: growing)	- Component, solution, service, Communication system, simulation, vertical and region
Public security and safety market (Pattern: growing)	- Component, solution, services, vertical and region

The types of customers for the DITHO are as follows:

- **Public and Private Security actors** include organisations such as crisis management and civil protection authorities, fire brigades, regulatory agencies, emergency health services, security managers, police forces, as well as private security organisations.
- **Municipalities services** interested in the APPRAISE DITHO module include for instance municipal police, local civil protection, urban security department, urban planning and design, transport-mobility, Tourism-Culture-Youth, and public spaces agents.
- **Critical venue operators** managing several millions (depending on focus) of sites that gather practically the majority of the EU population throughout the year Such venues include: Cultural activities (cinema, live performances or cultural sites), , Live performances (theatre, concerts, ballet), Cultural sites (historical monuments, museums, art galleries or archaeological sites), Closed Public Venues (Malls, Exhibitions), Cruise Ships, Hotels & Resorts, Airports, Train and Metro Stations, Sea Ports, etc
- **Authorities** – FCT Organisations and Policy Making Entities: EU agencies: Europol, Eurojust, Frontex, CEPOL, EU-LISA, EU Institutions such as European Parliament.

- SMEs, Industrials, integrators, consultants will exploit the platform to create addition tools or new services.

STAKEHOLDERS

Besides the above-mentioned customers, who also act as stakeholders, the following additional stakeholders have been identified:

- Research institutes: active in the field of soft target protection, can be interested in exploiting the DITHO for their research activities.
- Transportation market
- Energy market

Based on the analysis above and the opportunities provided by these growing markets, the priorities for the DITHO module would be on the Physical site security and on the public security and safety markets. In terms of geographical focus, CS GROUP will first target European actors, with the possibility to extend to the North America and Asia.

4.5.1.3 COMPETITORS

The DITHO and more specifically the Crimson product already present on the market, is a Physical security information management system. CS Group has identified 12 competitors on European level, among which can be found Genetec, Airbus Defence and Space, Iconics and GENESIS 64. The areas of expertise of these competitors vary from Event organisation, through finance, transportation, Smart cities, health, to Culture. On an international level 18 companies have been identified as competitors.

Although the urban security market strongly needs solutions meeting LEAs and security organisations' needs, currently there is no integrated solution available in the market offering all the features of APPRAISE. Very recently, supervision and C2 providers have adopted the DT concept for the management of public space protection and rescue operations (Genetec, Airbus Défense & Space, Iconics' GENESIS64, CS' Crimson), often adapting systems from the military or industrial domain to public space protection. There is still no effective solution for vulnerability assessment and planification, which is the reason of the extremely positive feedback the STEPWISE prototype received from practitioners. From the preliminary analysis of APPRAISE partners, APPRAISE is able to differentiate itself firstly by proposing a solution which is specific to the protection of urban soft targets and public spaces and that integrates SELP and population/traffic aspects and enables intuitive creation of scenarios. .

4.5.1.4 PARTNERS AND PROVIDERS

The DITHO with the related components developed under APPRAISE can be commercialised without any additional providers. When it comes to partnerships, it is envisageable to team up with providers of specific services and tools, in order to build a more complete and competitive offer.

4.5.1.5 SWOT ANALYSIS

INTERNAL FACTORS	
STRENGTHS	**WEAKNESSES**
• Crimson is an open platform • Important amount of field knowledge gathered over the years • Reputation and experience in several areas (FRs, site protection) • Cybersecurity component can lead to new markets or widen existing ones • Crisis management competence	• Amount of sensors already integrated • Amount of legacy systems to support, including interoperability

EXTERNAL FACTORS	
OPPORTUNITIES	**THREATS**
• Widen the use among LEAs • Build a more comprehensive tool suitable for soft target protection • Integrate functionalities valued by public/private end-users and gain their confidence.	• Competition • Available budget • Legal framework

5 CONCLUSIONS

This deliverable has presented the market analysis for the entire APPRAISE platform, as well as each individual component that can potentially be commercialised by the relevant partner. Some modules, being developed by research centres have an important value for the project and the whole platform, despite the fact that there is no dedicated market analysis at this stage. The analysis also shows that there is a growing demand for the multiple APPRAISE modules, as such, but also for a holistic and flexible platform at the one developed in APPRAISE.

The main market segments targeted by the APPRAISE platform are the cybersecurity and the physical security markets, along with the Global smart cities market. Furthermore, the platform is addressing the Cyber and Physical security market that emerging to answer the growing need to have a holistic and comprehensive approach when it comes to the cyber and physical soft target protection aspects. Furthermore, each APPRAISE tool developed to address a specific security need can be deployed separately, thus targeting a particular market segment, answering its single needs. In terms of priority markets the APPRAISE platform and the majority of the modules are mainly targeting the following markets: European Union countries, North America and Asia.

The document presents the vision of each partner and the project as a whole in November 2022. Until the end of the project the market trends and evolution will be closely followed, to better answer current and evolving needs in terms of soft target protection.

6 REFERENCES

[1] "Cybesecurity and Physical Security convergence," [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021_0.pdf.

[2] "Physical manipulation/damage/theft/loss," [Online]. Available: https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/etl-review-folder/etl-2020-physical#%5B%7B%22num%22%3A30%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22XYZ%22%7D%2C0%2C720%2C0%5D.

[3] "Physical securtiy Market size," [Online]. Available: https://www.alliedmarketresearch.com/physical-security-market.

[4] "Cyber Secutiy Market size," [Online]. Available: https://www.grandviewresearch.com/industry-analysis/cyber-security-market.

[5] "Smart cities Market by Focus Area," [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/smart-cities-market-542.html.

[6] "Threat Detection Systems Market Forecast to 2027 - Covid-19 Impact and Global Analysis - by Type; Application and Geography - MarketWatch," [Online]. Available: https://www.marketwatch.com/press-release/threat-detection-systems-market-forecast-to-2027---covid-19-impact-and-global-analysis---by-type-application-and-geography-2022-11-02.

[7] "Video Surveillance Market by System Type," [Online]. Available: https://www.alliedmarketresearch.com/Video-Surveillance-market.

[8] "Biometrics Market Size, Share, Trends and Forecast 2022-2027," [Online]. Available: https://www.imarcgroup.com/biometrics-market.

[9] "The top 10 biggest companies in video surveillance," [Online]. Available: https://www.asmag.com/showpost/31985.aspx.

[10] "ISO 22311:2012(en)," [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso:22311:ed-1:v1:en.

[11] "ISO/IEC 30137-1:2019(en), Information technology — Use of biometrics in video surveillance systems — Part 1: System design and specification," [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:30137:-1:ed-1:v1:en.

[12] "ISO - ISO/IEC JTC 1/SC 42 - Artificial intelligence," [Online]. Available: https://www.iso.org/committee/6794475.html.

[13] "EC Videosurvellance policy," [Online]. Available: https://commission.europa.eu/select-language?destination=/node/9.

[14] "Anomaly Detection Market Analysis, Growth, Size (2022 - 27) (mordorintelligence.com)," [Online]. Available: https://www.mordorintelligence.com/industry-reports/anomaly-detection-market.

[15] "Countering Threats," [Online]. Available: https://www.cpni.gov.uk/system/files/documents/40/14/c-uas-branded-doc-public-V4.1.pdf.

[16] "Sapient Autonomous Sensor System," [Online]. Available: https://www.gov.uk/guidance/sapient-autonomous-sensor-system.

[17] "The global video analytics market is projected to grow from $6.35 billion in 2022 to $28.37 billion by 2029, at a CAGR of 23.8% in forecast period, 2022-2029... Read More at:- https://www.fortunebusinessinsights.com/industry-reports/video-analytics-marke," [Online].

[18] "Water View," [Online]. Available: https://www.waterview.ai/.

[19] "Market Research Future," [Online]. Available: https://www.marketresearchfuture.com/.

[20] "marketsandmarkets," [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/threat-intelligence-security-market-150715995.html?gclid=CjwKCAiAoL6eBhA3EiwAXDom5uoAjlDdlrI6fQhtEEAinUOCzo38Pfp_tpzt7wALxVvQ1rL2WQPTmBoCZToQAvD_BwE.

[21] "Geospatial Analytics Market by Component, Solution (Geocoding and Reverse Geocoding and Thematic Mapping and Spatial Analytics), Service, Type, Technology, Deployment Mode, Organization Size, Application, Vertical and Region - Global Forecast to 2027," [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/geospatial-analytics-market-198354497.html.

[22] "DATA DISCOVERY MARKET - GROWTH, TRENDS, COVID-19 IMPACT, AND FORECASTS (2022 - 2027)," [Online]. Available: https://www.mordorintelligence.com/.

[23] "Global Web Scraper Software Market: Market Segments: By Type ; By Application ; and Region – Analysis of Market Size, Share & Trends for 2014 – 2019 and Forecasts to 2030," [Online]. Available: https://www.globenewswire.com/news-release/2022/07/12/2477949/0/en/Global-Web-Scraper-Software-Market-Market-Segments-By-Type-By-Application-and-Region-Analysis-of-Market-Size-Share-Trends-for-2014-2019-and-Forecasts-to-2030.html.

[24] " Most popular social networks worldwide as of January 2022, ranked by number of monthly active users," [Online]. Available: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/.

[25] "OSINT Market & Technologies - 2020-2026," [Online]. Available: https://homelandsecurityresearch.com/reports/osint-market-national-security-defense-homeland-security-private-sector-public-safety/.

[26] "Global Web Scraper Software Market: Market Segments: By Type ; By Application ; and Region – Analysis of Market Size, Share & Trends for 2014 – 2019 and Forecasts to 2030," [Online]. Available: https://www.globenewswire.com/news-release/2022/07/12/2477949/0/en/Global-Web-Scraper-Software-Market-Market-Segments-By-Type-By-Application-and-Region-Analysis-of-Market-Size-Share-Trends-for-2014-2019-and-Forecasts-to-2030.html.

[27] " OSINT Market: What Is It and What Potential Does It Have," [Online]. Available: https://www.molfar.global/en-blog/osint-market-what-is-it-and-what-potential-does-it-have.

[28] "Security Surveillance Market Share, Size Global Industry Key Tactics, Historical Analysis, Segmentation, Application, Technology, Trends and Opportunities Forecasts to 2027," [Online]. Available: https://www.wicz.com/story/46837436/Security-Surveillance-Market-Share,-Size-Global-Industry-Key-Tactics,-Historical-Analysis,-Segmentation,-Application,-Technology,-Trends-and-Opportunities-Forecasts-to-2027%20.

[29] "Social Media Analytics Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)," [Online]. Available: https://www.researchandmarkets.com/reports/4472756/social-media-analytics-market-growth-trends.

[30] "Global Social Networking Platforms Market (2021 to 2026) - Featuring Facebook, Pinterest and Twitter Among Others," [Online]. Available: https://finance.yahoo.com/news/global-social-networking-platforms-market-110300542.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&gu

ce_referrer_sig=AQAAAJ1FXdA0LnNPa6NARzYkIW4wgQpY5-2RJz9sVNylUgWPDxAyNEaQcAbbZMn_MTvqyaHKOdg1X98mPeWkhLLhr9.

[31] "Risk Analytics Market - Growth, Trends, COVID-19 Impact, and Forecasts (2021 - 2026)," [Online]. Available: https://www.researchandmarkets.com/reports/4535743/risk-analytics-market-growth-trends-covid-19.

[32] "Risk Analytics Market Analysis," [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/risk-analytics-market-210662258.html.

[33] "Enterprise Data Management Market Size, Share, & Trends Analysis Report by Component (Software, Services), by Services (Managed Services, Professional Services), by Deployment, by End Use, by Region, and Segment Forecasts, 2022-2030," [Online]. Available: https://www.researchandmarkets.com/reports/5415471/enterprise-data-management-market-size-share.

[34] G. V. E. Botanni, "Augmented reality technology in the manufacturing industry: A review of the last decade," [Online]. Available: https://doi.org/10.1080/24725854.2018.1493244.

[35] "European Commission, Directorate-General for Communications Networks, Content and Technology, Vigkos, A., Bevacqua, D., Turturro, L., et al., VR/AR Industrial Coalition : strategic paper, Publications Office of the European Union, 2022," [Online]. Available: https://data.europa.eu/doi/10.2759/197536.

[36] " Physical Security Market by Component (System, Services), by Systems Type (Physical Access System, Video Surveillance System, Perimeter Intrusion and Detection, Physical Security Information Management, Others), by Service Type (Access Control as a Servi," [Online]. Available: https://www.alliedmarketresearch.com/physical-security-market.