Sustaining Global Defence Productions

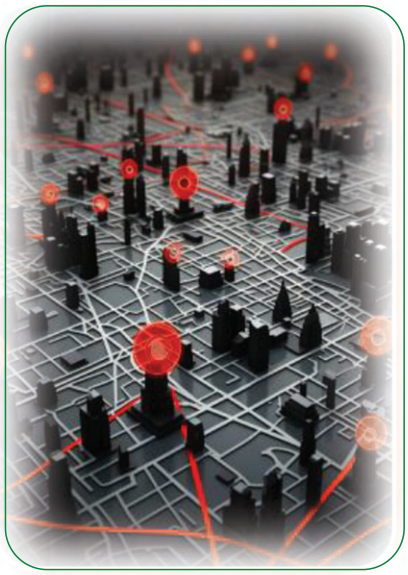
‘Sustaining Defence Production, and enhancing transfer of technology.’

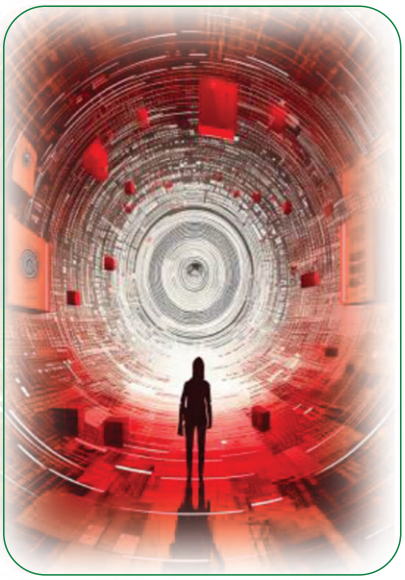
Digital intelligence

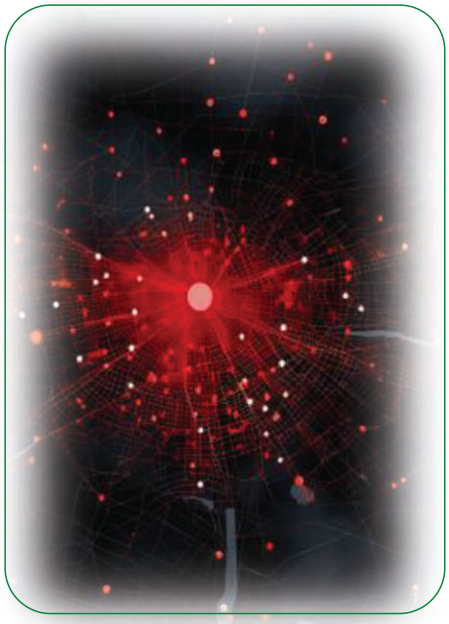

Provide the best of
DICON D7G Company
Arms Industry,
Stocks and Production

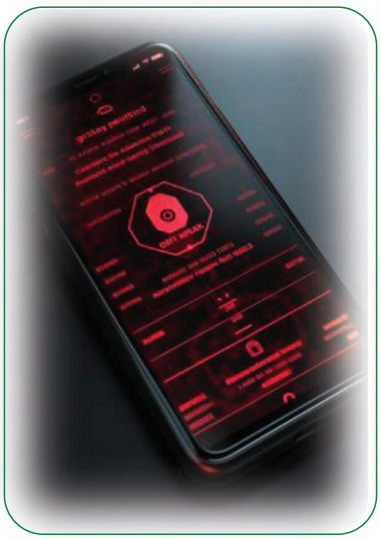
Digital Intelligence

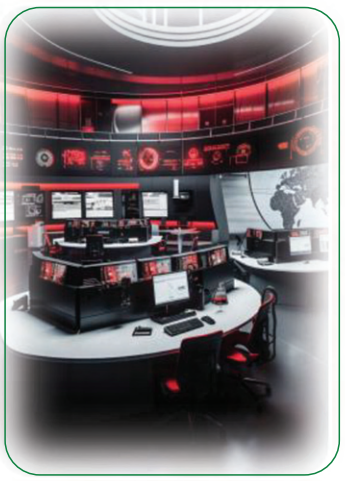
Products Overview











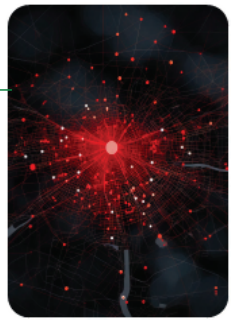
Digital Intelligence

Our Cutting Edge Solutions

Our Cutting Edge Solutions

Location Intelligence

Utilizes geospatial data for enhanced situational awareness and informed decision-making in their operations.



LBS

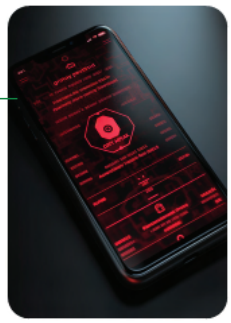
Leverages geographical data to track and analyze the location of devices or individuals for operational purposes.

OSINT

Unleash the potential of our OSINT solution for comprehensive information gathering and analysis, providing actionable insights for strategic decision-making and enhanced security.

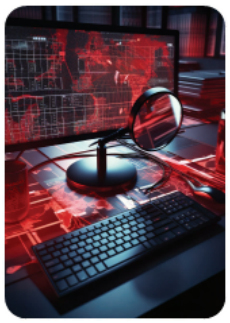
CCTV AI Module

Utilizes advanced algorithms to identify and track faces or vehicle license plates, aiding in surveillance and security applications.



Secure Messenger

Ensures confidential communication, protects sensitive data, and maintains operational security amidst evolving digital threats.

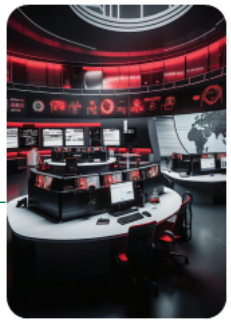


Digital Forensics

Extract, analyze, and leverage digital evidence crucial for uncovering threats, understanding adversaries, and safeguarding national security.

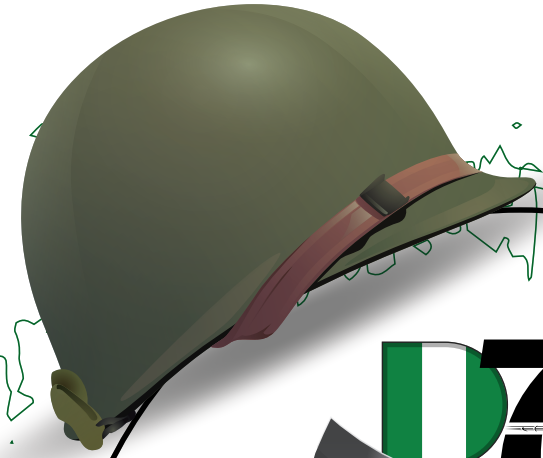
Surveillance & Counter-Surveillance

Protects against adversaries' monitoring, safeguarding classified information and operations.



Cybersecurity

Cybersecurity products are vital defenses against digital threats, employing technologies like firewalls and antivirus software to safeguard systems and data from unauthorized access and attacks.



Sustaining Global Defence Productions

A Revolution in Geospatial Technology through an Innovative Crowd Intelligence System; Pioneering Counter Terrorism and Crime Prevention.

Dicon D7G creates behavioral analytics models that enable us to analyze the digital footprints of anonymous devices based on their movements and behaviors. These models reveal incredibly intelligent patterns.

Why DICON D7G

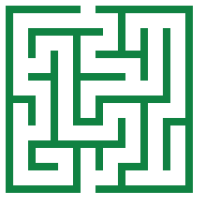
Why DICON D7G

Investigate

Monitor

Protect

Predict & Prevent



DICON D7G

Detecting & Combating most types of crime

- **Organised Crimes**
- **Terrorism**
- **Financial Crimes**
- **Border Security**
  (Human trafficking, Weapons Supply, ...)
- **Critical Infrastructure Security**
- **Natural Disasters**
- **Espionage**

DICON D7G

Organized crime

- Drug Trafficking
- Drug dealing
- Human Trafficking
- Kidnapping
- Banditry

Counter-Terrorism

- Identify key players
- Identify their locations
- Terrorists' groups with sudden movements
- Identify threat patterns
- Track Terrorists' activities
- Uncover hidden trends
- Discover relationships

Critical infrastructure Security

- Real time insights into the status of critical infrastructure (Pipelines, Airports, Embassies,...)
- Illegal activities interception
- Predictive analysis
- Proactive threat detection & protection
- Logistics tracking

Financial Crimes

- TBML
- TBTF
- Money Laundering
- Corruption
- Fraud
- Tax Evasion

Financial Crimes

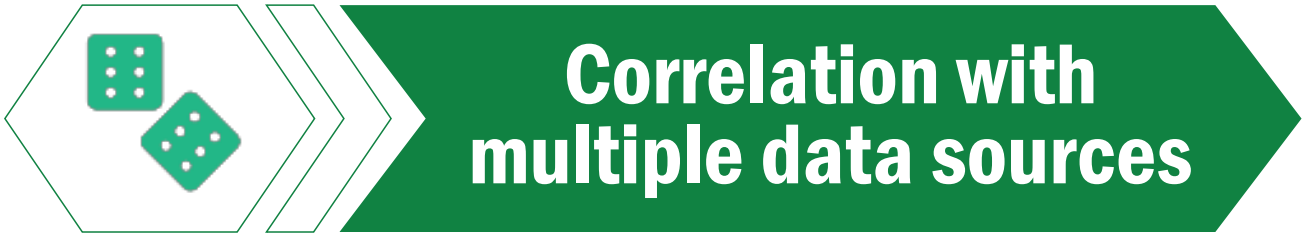
- Detect suspicious behavior at onboarding
- Mitigate transaction fraud and slash false positives
- Prevent account takeovers & account update fraud
- Investigating Corruption Networks
- Identifying Asset Locations
- Tracking Financial Flows

Border Security

- Protect your borders 24/7 and get alerted by any trespassers
- Identify & protect critical premises (geofencing)
- Tracing illicit supply chains (weapons, ...)
- Demonstrate trafficking routes
- Identify smugglers and their inter countries activity

DICON D7G Concept

DICON D7G Concept



Friendly graphical user interface

- Synchronize different platforms among agencies
- Different Data modules under ONE suite
- No need for technical skills

Offline system

- Standalone server.
- No internet connection is needed.

Global visibility

- Data insights beyond borders.
- Manage a large amount of data (Up to 100,000 application feeding mobility Data Daily Integration of 50 billion records...).
- Data includes almost all countries.
- No need for traditional cooperation with local service providers.

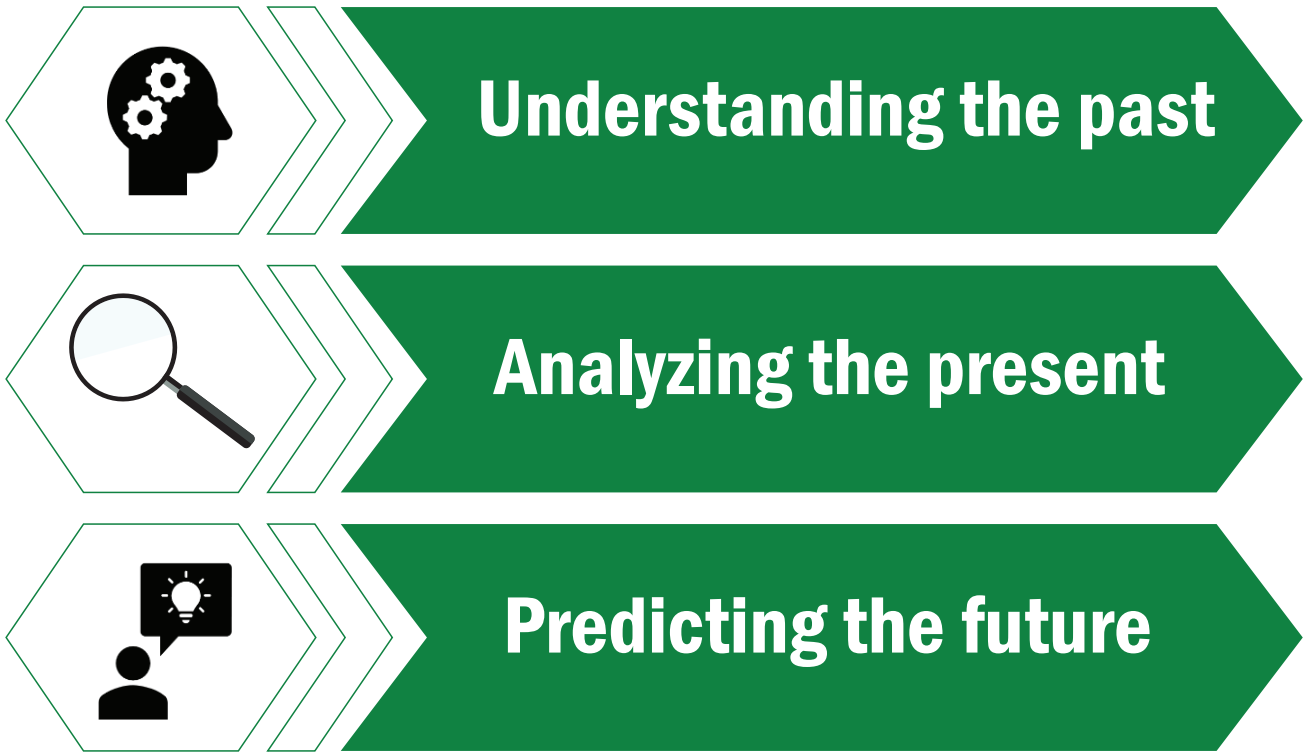
Investigator's ability to achieve technical tasks

- No need for sophisticated QUERIES.
- The investigator can do everything.
- Imagination is the limit.
- Reduce your circle of confidentiality.

Technology, Big Data & AI

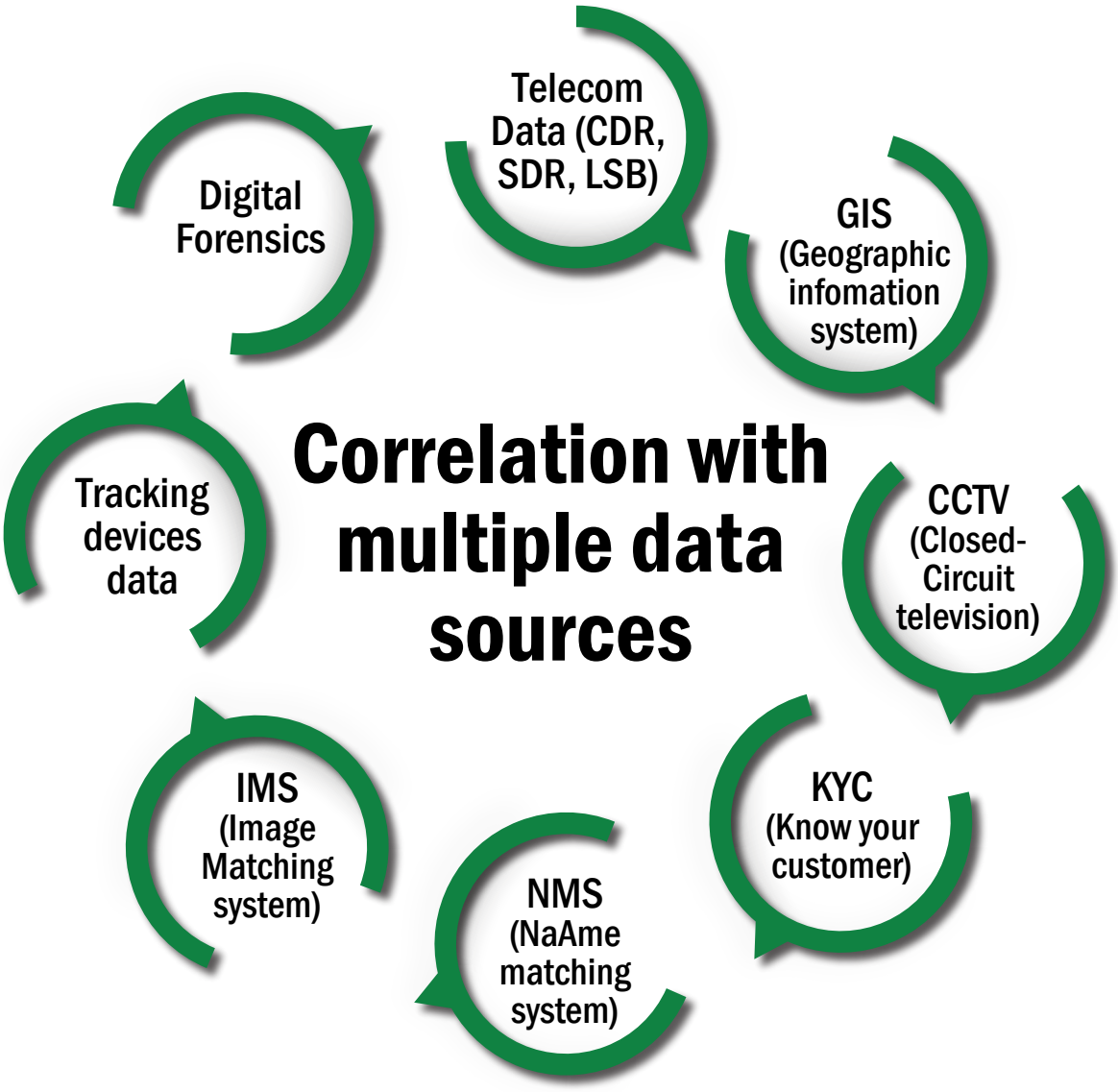
Handling	Handling structured and unstructured types of data
Ingesting	Ingesting the large amount of data in a measurable time
Executing	Executing any query or scenario in matter of seconds
Performing	Performing complex predefined scenarios in the background
	Flagging suspicious devices or entities
Providing	Providing alerts and daily threat analysis reports

Navigating in time:
Backward & forward investigations

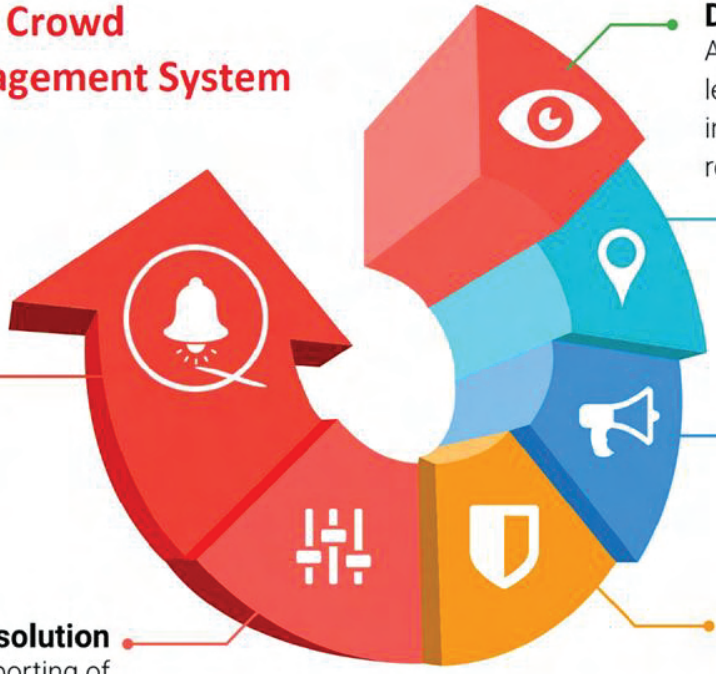


Control access to information

- Restrict Access to sensitive areas.
- Audit trail record.
- Multiple factor authentication (biometrics).



Data Crowd
Alerts Management System



DETECT - Event/Incident Detection
AI technology with machine learning is used to detect incidents and trigger responses

LOCATE - Analysis & Propagation
Analyzes data collected by human or AI technologies and shared with appropriate devices and resources

ACT - Alerts Delivery
Uses pre-designated groups to send alerts and notify resources, any device, any where

RESPOND - Event Management
Manages delivery of alerts and messages and responses with secure two-way messaging

FOLLOW-UP -Reassure & Audit Trail
Secure with audit trail, accelerated and proactive crisis response to save lives and protect assets

MANAGE – End-to-end solution
Management and reporting of IoT device. Device profile and content management with performance analytics

DICON D7G Alert management

Data Transfer through online platform (gcp, aws,...)

Downloading Data from Private Clouds

Cloud

No connection needed between

VCIS Data Servers and deployed platforms

DICON D7G Data Services

Law Enforcement Agency

LBS Active & Passive

LBS Active & Passive

Active

- Locate specific targets (Usually Up to 50+ targets)
- The accuracy is between 50-200 meters
- Is able to obtain the location of specific targets only
- NO Previous Historical Records

Passive

- Obtain all subscribers location
- Visualize on a dynamic map
- The accuracy is between 25-200 meters
- Detect whether the user is inside the house or in an open space

1

Location Accuracy

Our product guarantees top-tier location accuracy, harnessing innovative methods for precise and reliable positioning.

2

Dynamic Maps

Revolutionize your navigation experience with our dynamic maps product, providing real-time updates and interactive features for seamless exploration.

3

Data Visualization

Experience the power of seamless data visualization with our product, enabling the comprehensive analysis of large datasets at once.

4

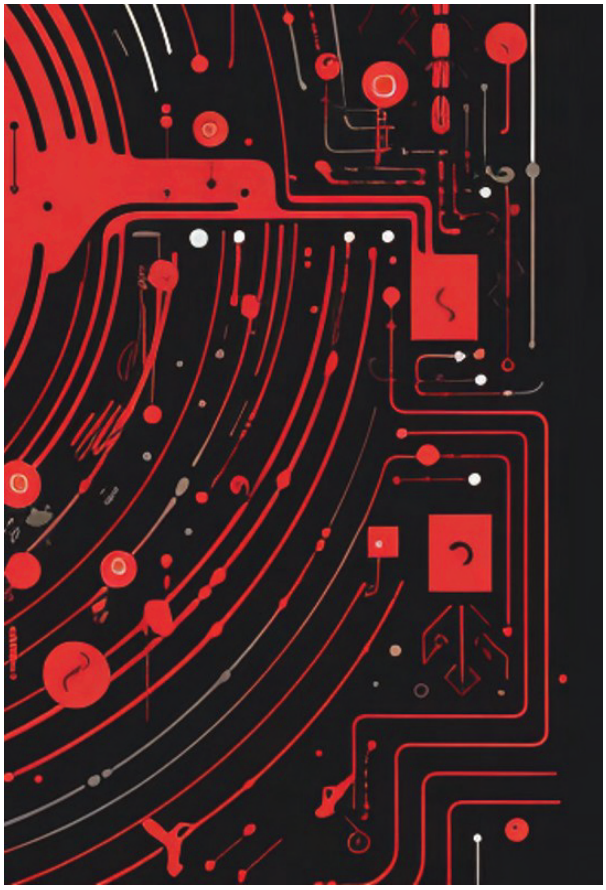
Load Efficiency

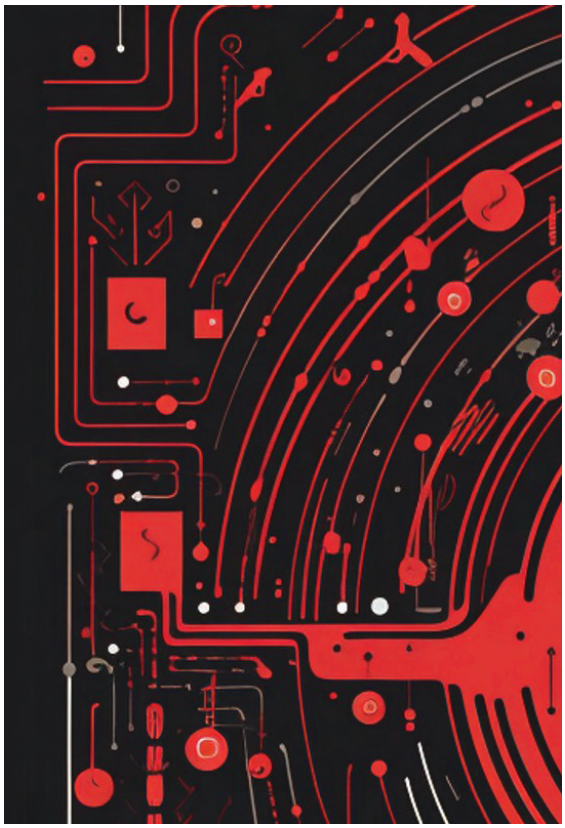
Our product excels in efficiently processing vast data volumes, ensuring swift and accurate insights for optimal decision-making.

OSINT Open Source Intelligence

Intelligence-Driven Decisions

Support decision-making, threat assessment, and strategic planning.





Analyze Large Sets of Data

Gather, analyze, and interpret publicly available data from Social Media, TVs, Websites, Newspapers, Chat Groups, Blogs & many others.

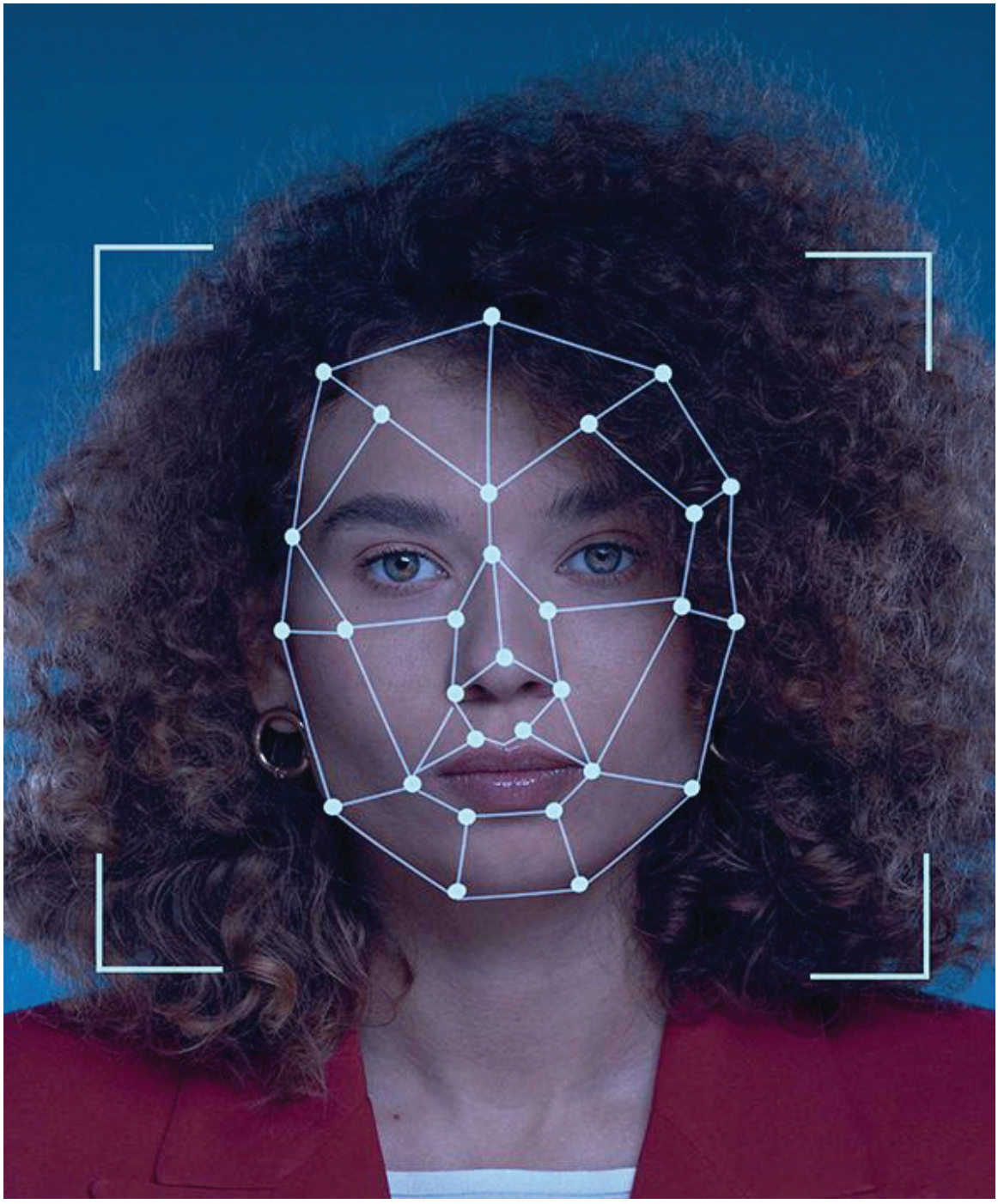
- **Real-time Insights:** OSINT offers current information for swift decision-making.
- **Threat Analysis:** Helps agencies proactively analyze potential risks and monitor activities.
- **Strategic Planning:** Contributes to effective strategies based on open source intelligence.
- **Timely Response:** Enables quick responses to emerging threats and incidents.
- **Collaboration:** Facilitates information sharing among security agencies and stakeholders.

OSINT Open Source Intelligence

CCTV AI Engine

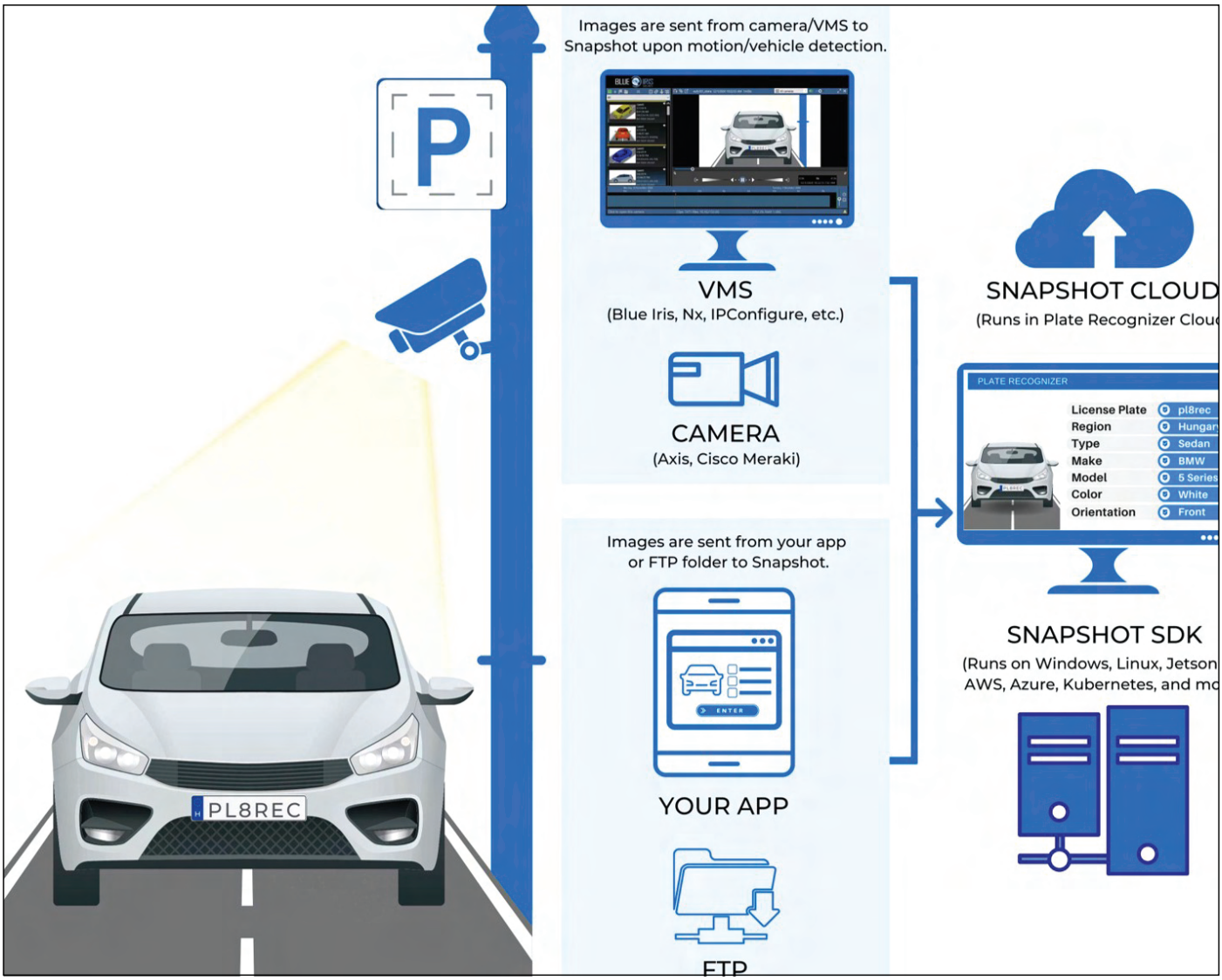
CCTV AI Engine

Face Matching & Recognition



- Enables search and reporting from vast amounts of video.
- Locates person of interest faster.
- Suitable for static and non-static video (mobile, CCTV, body worn etc.).
- Imports video with faces present.
- Detects faces in video & images quickly.
- Matches faces to suspect list.
- Exports out all faces found in video quickly.

ALPR
(Automatic License Plate Recognition)



ALPR System assists in:

- Tracking Suspects.
- Identifying and locating vehicles involved in criminal activities.
- Monitoring and tracking vehicles crossing international boundaries.
- Analyzing patterns, tracking vehicle routes, and identifying associations between different vehicles.
- Identifying stolen vehicles, unregistered cars, or vehicles linked to wanted individuals.
- Threat detection by flagging vehicles associated with potential security risks.

Secure Messenger

100%

Your Own The Code

Our product stands out by offering full ownership of the source code, granting users unparalleled control and adaptability. With the ability to customize and enhance the software independently, businesses gain flexibility, security, and long-term value. This unique feature ensures a strategic advantage, empowering users to shape the product according to their evolving needs.

100%

Your Own Infrastructure

Our product is uniquely hosted on self-owned infrastructure, guaranteeing users a secure, reliable, and fully controlled environment. With increased data privacy and reduced external dependencies, this approach not only ensures optimized performance but also instills confidence in users that their operations are within their complete control.

100%

Our product employs military-grade encryption, employing state-of-the-art algorithms to secure sensitive data with maximum effectiveness. Users can trust that their information is protected at the highest level, providing peace of mind and robust security against potential threats.

Mobile Forensics

- Extract data from mobile devices
- Recover deleted data
- Crime investigation
- Bypass locked phones
- Preserve Evidence

Computer Forensics

- Extract data from computers laptops and storage media
- Recover deleted data
- Crime investigation
- Bypass locked devices
- Detect Encryption and User Activity
- Preserve Evidence
- Malware Analysis

Mobile Forensics
Computer Forensics

Cloud Forensics

Cloud Forensics

- Crime investigation
- Extract data from online & Social Media
- Backups
- Preserve Evidence
- Accounts
- Recover & Download Data from Cloud
- Recover deleted data
- Find links between multiple devices

Vehicle Forensics

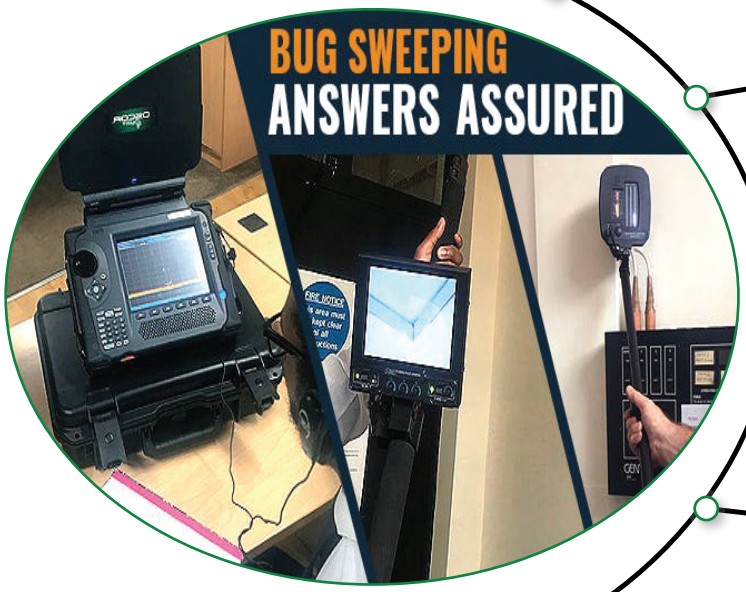
Vehicle Forensics

- Preserve Evidence
- Extract data from Vehicles
- Crime investigation
- Recover traces and routes
- Event reconstruction

Technical Surveillance

- Lazer microphone
- Audio and Video Recorders
- Network Interception Equipment & DPI
-
- Covert Listening Devices (Bugs)
- Hidden Cameras
- GPS Trackers

Counter-Surveillance



- Jammers
- Cellular Signal Detectors
- Bug Detectors/Sweepers
- Camera Detectors/Sweepers
- Spectrum Analyzers
- Wireless Signal Scanners

SIEM

Security information and event management

Components of SIEM

Data Collection

- Logs from diverse sources (firewalls, antivirus, servers, etc.).
- Network traffic analysis.

Normalization

- Standardizes and normalizes data for consistency.

Correlation

- Identifies patterns and relationships between events

Alerting

- Generates real time alerts for potential security incidents

Threat Detection

- Early detection of security threats and incidents.

Incident Response

- Enables quick and effective response to security incidents

Compliance Management

- Facilitates adherence to industry regulations and standards

Forensic Analysis

- Provides detailed analysis for post investigations.

Why SIEM Matters

EDR

Endpoint Detection & Response

Advanced Threat Detection

Identifies and responds to sophisticated threats Examines the reputation of files and processes, identifying potential threats based on historical data and behavior.

Reduced Dwell Time

* Implements automated response actions to minimize manual intervention and reduce the time it takes to neutralize threats.

* Proactively searches for threats on endpoints, helping to identify and mitigate potential risks before they escalate.

Endpoint Visibility

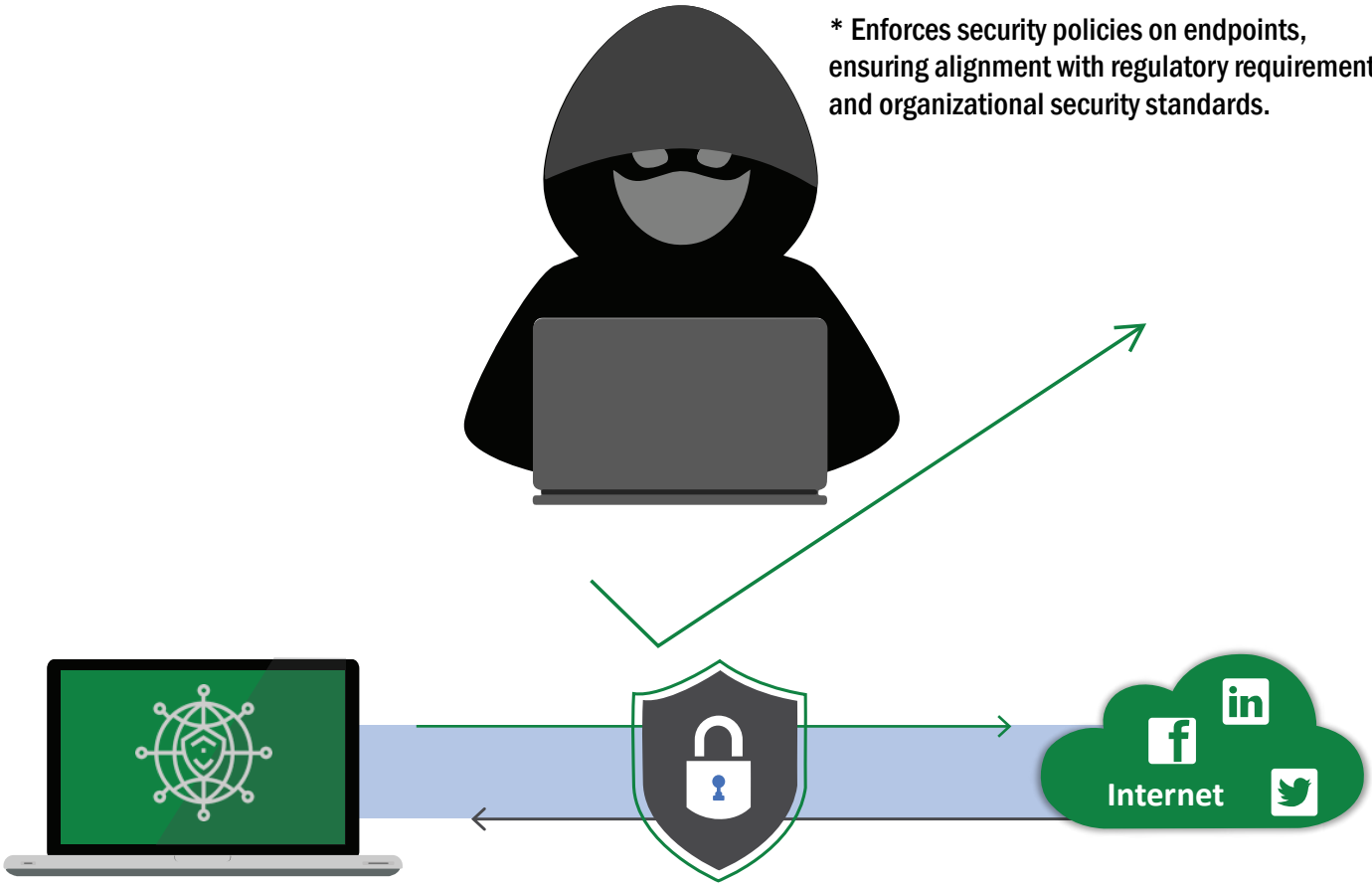
* Maintains an updated inventory of all endpoint devices, providing a comprehensive view of the organization's attack surface.

* Analyzes user behavior on endpoints, detecting anomalies and potential insider threats through advanced analytics.

Compliance Assurance

* Generates detailed audit trails of endpoint activities, aiding in compliance audits by providing a verifiable record.

* Enforces security policies on endpoints, ensuring alignment with regulatory requirements and organizational security standards.



Penetration Testing

Penetration Testing

Objective: Identifying Weaknesses

Systematically uncover vulnerabilities in software, hardware, and network configurations. Prioritize weaknesses based on potential impact and exploitability.

Approaches: Diverse Testing Methods

Black Box Testing:
Simulates external attackers with no prior knowledge of the target system.

White Box Testing:
Assesses the system with full knowledge of internal architecture and code.

Gray Box Testing:
Strikes a balance, providing partial knowledge for a realistic perspective.

Value Proposition: Proactive Security Measures

Risk Mitigation:
Prioritize and address high-risk vulnerabilities.

Compliance Adherence:
Support regulatory compliance with effective security controls.

Trust Building:
Demonstrate commitment to security, building trust with clients and stakeholders.

Process: Step-by-Step Exploration

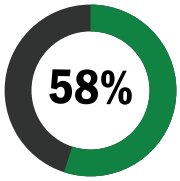
Planning and Reconnaissance:
Define scope, gather information, and understand the target environment.

Gaining Access:
Attempt to exploit vulnerabilities and gain unauthorized access.

Evaluate impacts, document findings, and provide detailed reports.

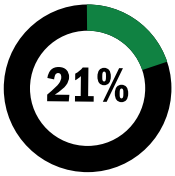
SOC Services

Security Operation Center



Skill Shortage

58% of organizations believe they have a problematic shortage of cybersecurity skills, impacting the effectiveness of their cybersecurity posture.



Outsourcing

21% of organizations outsource their SOC functions partially or entirely to third-party providers.

$215 Billion

Cybersecurity Spending

Worldwide spending on information security and risk management technology was projected to reach $215 billion in 2024, indicating a continued increase in investment.

Outsourced SOC Benefits

Cost Efficiency:
* Avoid upfront costs for infrastructure and technology.
* Benefit from economies of scale and shared resources.

Access to Expertise:
* Tap into diverse cybersecurity skills and experience.
* Ensure 24/7 monitoring and response with dedicated professionals.

Advanced Technologies:
* Access state-of-the-art cybersecurity tools and technologies.
    * Ensure regular updates to combat evolving threats effectively.

Focus on Core Business:
* Emphasize core business functions with internal teams.
* Mitigate security risks with dedicated experts, fostering business growth.

Virtual CISO

V C I S O

Cybersecurity Leadership Unleashed.

1. Leverage seasoned cybersecurity experts for strategic direction.
2. Develop and implement a risk management strategy aligned with your organization's specific needs.
3. Access CISO-level expertise without the cost of a full-time executive.
4. Swiftly deploy strategic cybersecurity measures with immediate effect.

Sustaining Global
Defence Productions

‘Technology Intelligence Portfolio’

Strategic Communications

RF-Monitoring & Direction Finding

Radio Frequency Monitoring is still a great challenge, especially in times of analog & digital waveforms, complex data coding and various other techniques used to transmit signals via electromagnetic waves.
We have not lost sight of the importance of RF and have extended the activities in modern RF Reconnaissance by using competitive COTS wideband receivers and Direction Finders.

Satellite Monitoring

Monitoring of commercial satellites with strategic and tactical systems is a steadily increasing business, and the actual portfolio of Inmarsat and Thuraya systems could be extended by VSAT systems as well as complex satellite analysis, showing the occupancy and free transponder channels.

Location Services (ADINT)

Unlock the power of geospatial data with a modular platform that transforms location intelligence into actionable insights for defense and intelligence (ADINT) operations. Designed to support mission-critical decision-making, it enables agencies to analyze high-risk zones, visualize threat patterns in real time, and implement predictive strategies. With advanced analytics and machine learning tools, this solution empowers security organizations to anticipate threats, optimize resource deployment, and enhance operational readiness through geolocation intelligence.

Public Opinion Exploitation Management

Public Opinion Exploitation Management (POEM)

POEM is an all-in platform solution designed to automate large-scale Social Media campaigns and influence public narratives. It allows users to create, distribute, and manage messages at scale, targeting influencers and countering opposing viewpoints with strategically timed content.

POEM utilizes sophisticated techniques – including mimicking human behavior through randomized messaging, customized hashtags/images, and the use of multiple smartphone devices with unique identifiers – to avoid detection by Twitter's algorithms. The system offers on-site installation for enhanced privacy and autonomy, alongside optional support packages for social media development and ongoing influence operations. POEM's core function is automated counter-messaging strategy processing, generating numerous tweets based on pre-defined parameters and text templates. It facilitates narrative planning, targeted messaging, early intervention in viral trends, and the ability to both refute or support influencer messages.

The system operates by remotely controlling Social Media apps on Android devices, simulating real user activity through randomized tweet generation, re-tweeting interactions, and subtle language modifications designed to evade bot detection – ultimately aiming to shape public opinion according to defined objectives.

Blockchain Analysis

There is a worldwide crackdown on money laundering and criminal-funded activities with regards to traditional currencies. Many criminals have turned to anonymous cryptocurrencies to finance their operations and launder money originating from illegal activity, taking advantage of the anonymity and encryption provided by the blockchain ecosystem.

Our Blockchain Analysis tool helps to correlate real-life events with blockchain data.

Starting the investigation from a Wallet ID or an IP address, investigators are able to track cryptocurrency transactions, money laundering attempts using mixing services, gambling activities, illegal marketplace transactions, ransomware earnings, topping of online wallets, clusters (groups of related cryptocurrency addresses) and much more.

Cyber Intelligence

Avalanche: Fortify Your Nation's Digital Defenses

Our innovative platform provides a unique capability to rigorously validate and strengthen your defenses against DDoS attacks and related malicious online activity. We offer advanced Cyber Drill simulations, security posture validation for critical infrastructure, and comprehensive penetration testing – all supported by a dedicated team of DDoS SMEs continuously developing cutting-edge techniques.
This technology can be utilized to disrupt harmful online activities such as disinformation campaigns, fraudulent websites, and forums used for terrorist coordination. This capability is coupled with operational security features like smoke screen implementation, ensuring a layered approach to protecting your nation's digital future.

Mobile Number de-Anonymizer

The 1-Click Solution enables the identification of mobile numbers associated with devices used by anonymous targets. This de-anonymization process occurs when the target clicks and browses a specially crafted Unmask URL while connected to mobile internet. It is effective across all mobile device platforms, including iOS and Android, as long as the device has direct internet access. The solution also works for mobile and desktop devices connected via 3G, 4G, 5G routers, tethering, or mobile hotspots, and even when devices are using data roaming. Notably, standard device updates or advanced security features such as "Lockdown Mode" do not prevent the de-anonymization process.

Tactical Communications

Portable Satellite Monitoring

The Tactical compact, mobile systems designed to receive and analyze signals from commercial satellites. These systems are typically used for applications like communications, surveillance, or data collection analysis. Unlike fixed satellite stations, portable units are lightweight and easy to deploy in remote or temporary locations, offering flexibility for field operations. They usually include a small satellite dish or antenna, a receiver, and processing equipment, often powered by batteries or portable generators.

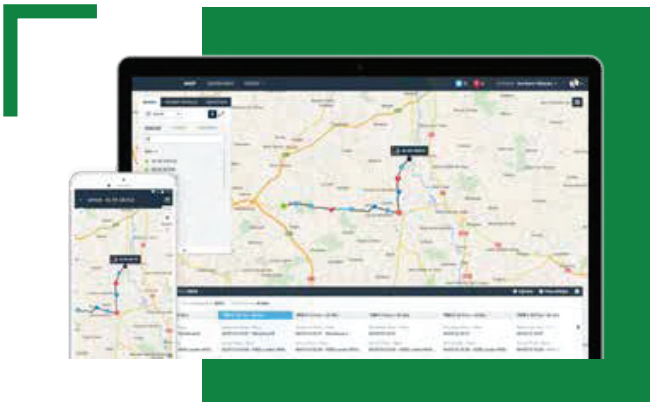
Technical Surveillance Systems

Covert Video-Audio Surveillance

Our range of Covert Video-Audio Surveillance involves the discreet monitoring, recording and transmitting of activity without the subject's knowledge. Commonly used by intelligence operations, this type of surveillance helps gather evidence or monitor suspicious behavior without alerting targets. Devices are often hidden in everyday objects, allowing them to blend seamlessly into the environment for maximum stealth and effectiveness.

Tracking & Tyre Deflaction

Tracker and Tyre Deflation systems are covert tools used in surveillance and law enforcement to monitor movements and discreetly immobilize targets. Trackers placed in Vehicles can be a great additions for Tyre deflation devices which are used to slowly or instantly deflate a vehicle's tires, helping to stop or delay its movement during operations. These tools are crucial in high-risk or sensitive missions requiring stealth and control.



Hides, Concealments & Deployment

Creating natural looking strong, durable and accessible hides for the concealment and deployment of cameras, microphones, batteries, RF antennas and other related surveillance equipment is often required by TSCM units

Audio Video Enhancement

Even with the highest quality of recording there are often background noises that need filtration, i.e. air-conditioning units, street noises, TVs, etc. We offer an optional section for audio filtration which not only filters but enables you to process all the recording as well as a storage facility. Furthermore, we have added an audio enhancement system suite to enable video recordings to be fine-tuned for ultimate quality and data storage.

Technical Surveillance - Vans/Cars

Our Bespoke Surveillance Vans and Cars are custom-designed vehicles equipped with advanced surveillance technology for covert operations.
These vehicles are tailored to meet specific operational needs and may include hidden cameras, audio recording systems, communication interceptors, and monitoring workstations.
Externally indistinguishable from regular vehicles, they allow operatives to conduct discreet surveillance, track targets, and gather intelligence without drawing attention. Commonly used by law enforcement, intelligence agencies, and private security firms, these mobile units provide a versatile and controlled environment for field operations

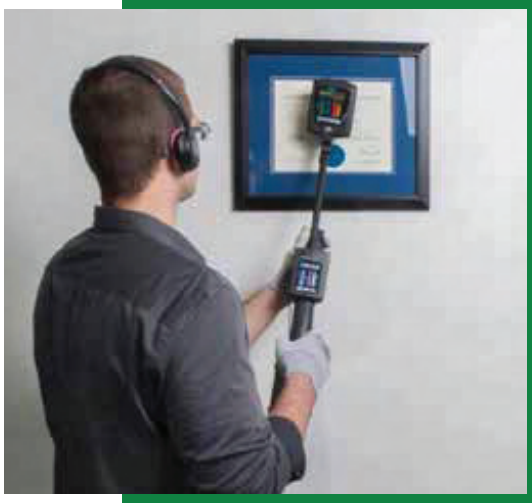
Covert Method of Entry

Tactical units require, in many cases, nondestructive entry, for example into hotel rooms or vehicles. We are able to offer the latest developments in lock-picking, RFID cloning, key duplication, safe opening, vehicle entry and alarm defeat. Training is available on the use of all tools.

Electronic Surveillance Command & Control Platform

A centralized Command and Control Centre, designed to track anything, anyone, anytime, anywhere. Our platform provides situational awareness and remote device management solutions where 1000s of end devices (trackers, cameras, phones, UAVs, etc.) can be visualized, linked and commanded and controlled.

Technical Surveillance Counter-Measures



Surveillance Counter Measure Equipment

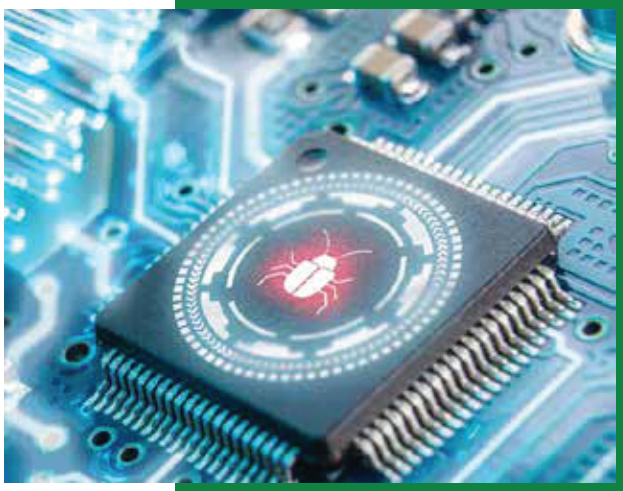
We offer many different spectrum analyzers for the Detection, Analysis, Classification and Localization of RF Signals between 8kHz and 8GHz.From the most advanced TSCM handheld spectrum analyzer that can capture the shortest signal transmissions to a fully integrated portable Spectrum Analyzer. These are specifically for professional countermeasures use with the highest possible technical specifications to ensure maximum detection capability.

Portable & Fixed WiFi Detection

Portable & fixed WiFi detection and localization solutions for detecting rogue WiFi base stations, analyzing WiFi networks, discovering connected devices, and finding them.

Pursuit is geared for portable scanning, as part of a TSCM sweep or a VIP protection forward team.

Vision is for fixed deployment and protection of sensitive sites, headquarters, and offices.



TSCM Training

A professional counter-surveillance team or so-called sweep-team needs good experience in modern surveillance electronics as well as top knowledge on how to operate equipment to detect and locate hidden electronics used to gather information for espionage.

We offer extensive training covering physical search, cable measurements, RF-sweeps, X-Ray & thermal inspection, telecom & IT-systems inspection andmore -- all in authentic espionage scenarios.

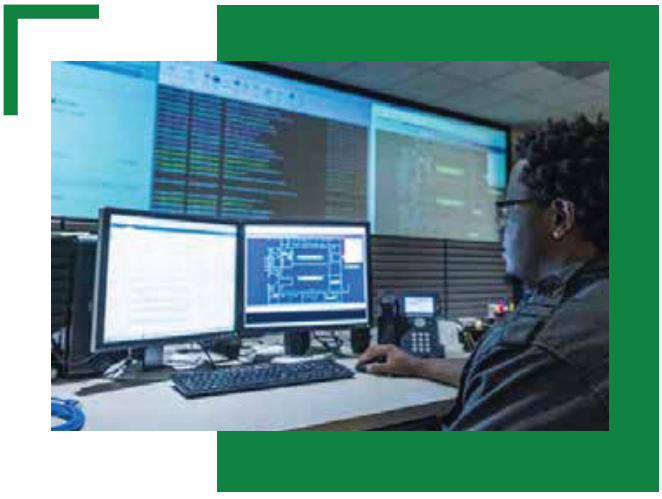
Specialized Security Solutions

VIP Mesh Communication

The Modular Rapid Deployment Surveillance System is a flexible, DC-powered solution designed for quick setup in the field. It supports up to 64 nodes within a secure, private wireless mesh network that operates independently of public telecom infrastructure. Engineered for real-time IP data, voice, and video transmission, the system ensures enhanced security and seamless situational awareness.
A dedicated app allows for easy management, control, and live video monitoring

GSM Secure Communications

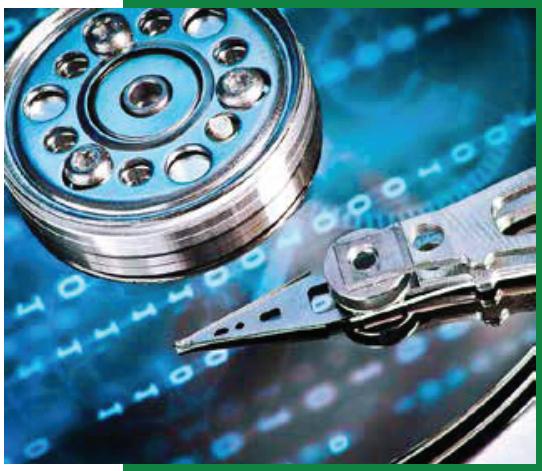
Secure Phone products offer strategic information security in mobile communications. Nowadays, there is a concern: of increased exposure to the risk of inteception. Unfortunately, cheaper equipment that is easier to use has made the interception of telephone calls accessible to a multitude of criminal players. To confront this, we offer secure mobile communications which are trustworthy, giving you encryption and device security in all vectors of approach, transforming your normal everyday phone into a customized hardened device with customized solution.



Secure App & Malware Detection

ARGOS offers a revolutionary approach to mobiledevice security for LEAs and government institutions. It operates externally, analyzing device activity without app installation to detect malware, encrypt communications, and restrict application usage – all while maintaining data control within your environment. Backed by decades of offensive security expertise, ARGOS provides flexible deployment options (on-premise, cloud, or portable WiFi kit) and real-time awareness through automated alarms, offering a robust defense against sophisticated mobile threats without the need for custom hardware.

Forensics Analysis



Computer & Mobile Forensics

In this digital age, law enforcement and intelligence agencies are faced with an increasing number of situations where digital evidence or electronic data play a crucial role in everyday operations. Establishing a capability to gather digital evidence and electronic data from PCs/Hard Discs or Mobile Phones can play a significant role in developing a more secure environment and improve the ability to meet those challenges from international terrorism and criminality. We offer Mobile Phone Forensics, HDD, SSD, flash drive recovery, unlock tools & password crackers and extensive Video & Audio Forensic tools.

Forensic Lab

The effectiveness of a digital forensic laboratory depends on the software, hardware and equipment used. For a digital investigation, it is necessary to provide a working environment equipped with different technical capabilities, such as a Forensic Workstation and a Centralized Investigation Server, in order to acquire data from suspect media. Furthermore, it is necessary to have a powerful system to process and analyze that media with different standalone software. We will build your laboratory around technically proven and established data recovery hardware and sophisticated digital software tools to create a highly effective operational facility

Laboratories on Wheels

A completely equipped state-of-the-art functioning mobile laboratory on wheels that is totally self-sufficient and comes with a range of fully configured systems that is always up-to-date. Each system is customized to suit the exact requirements of each customer. Each mobile Laboratory is equipped with unique worldwide recognized Swing Racks to protect sensitive equipment that is isolation and technology proven to work in all types of climatic conditions.

Data Fusion Platform

Information Fusion C&C Center

The latest in intelligence-related metadata analytics makes the life of analysts much easier, as has been shown with our IFP – Information Fusion Platform. It started as a real analytical SIGINT platform, and currently can pull metadata out of other sensor systems such as OSINT & COMINT, providing a cutting-edge and comprehensive analytical application. The solution is also scalable and modular allowing for quick and easy adaptation to a client's needs or budget constraints. All types of data sources can be connected/integrated.

Turnkey Training

Turnkey Training for Technical & Operational Intelligence Departments

This offering provides comprehensive, turnkey training programs specifically designed for technical and operational intelligence departments. The curriculum is tailored to equip personnel with the skills needed to effectively utilize advanced intelligence gathering techniques and technologies

Operational Training & Mission-Based Services

We deliver world-class operational training and mission-based services globally (UK/Europe, MEA, or Asia) or at your facilities. Our specialist programs are led by experienced instructors – former Special Forces, Government, Law Enforcement, and Technical Engineering Specialists – ensuring clients achieve mission-critical success through practical application and ongoing support

Marine Security & Protection

Marine smuggling and dark vessels

Introduction

Criminals have become increasingly adept at taking advantage of people's need to move and their limited choices for doing so, to generate enormous illicit profits by facilitating unsafe migration. Migrant smuggling has been the focus of significant international laws and policies owing to the particular dangers posed to migrants smuggled in perilous conditions at sea. Smuggling by sea has been detected in several regions, including the Gulf of Aden, the Pacific Ocean, the Bay of Bengal, the Andaman Sea and the Mediterranean Sea. Smugglers often increase their profits by reducing safety and keeping conditions poor on board, which usually means cramming people into unseaworthy, disposable vessels.

Tracking vessels with automatic identification systems (AIS)

International waters are governed by the International Maritime Organization (IMO). The IMO requires all ships to use an automatic identification system (AIS). AIS uses the vessel's GPS or sensor built in to the AIS unit to transmit information including:

* the vessel's name, unique marine identity number and call sign
* the type of vessel (fishing, cargo or passenger)
* the vessel's size
* the vessel's position on the sea
* its course of travel and speed.

The AIS broadcasts the vessel's position continuously – every 2–12 seconds in order to avoid collisions at sea. Satellites pick up this information and relay it to ground stations, so even vessels in remote parts of the ocean are tracked.

Dark vessels

Vessels that do not want to be tracked switch off their AIS systems. They 'go dark' and are known as dark vessels. The ships may also be involved in transferring illegal goods or smuggling drugs or people. All illegal activities are carried out by dark vessels.

Unlike registered boats, dark vessels don't have identification systems so they can't be tracked. With radar imaging, every boat on the ocean becomes visible, regardless of weather conditions or restricted waters. Cross-checking against registered signals reveals which ships don't belong.

To be able to identify and track dark vessels an intelligent system comprised of Radar, a Frequency direction finder and an AIS transponder is mandatory.

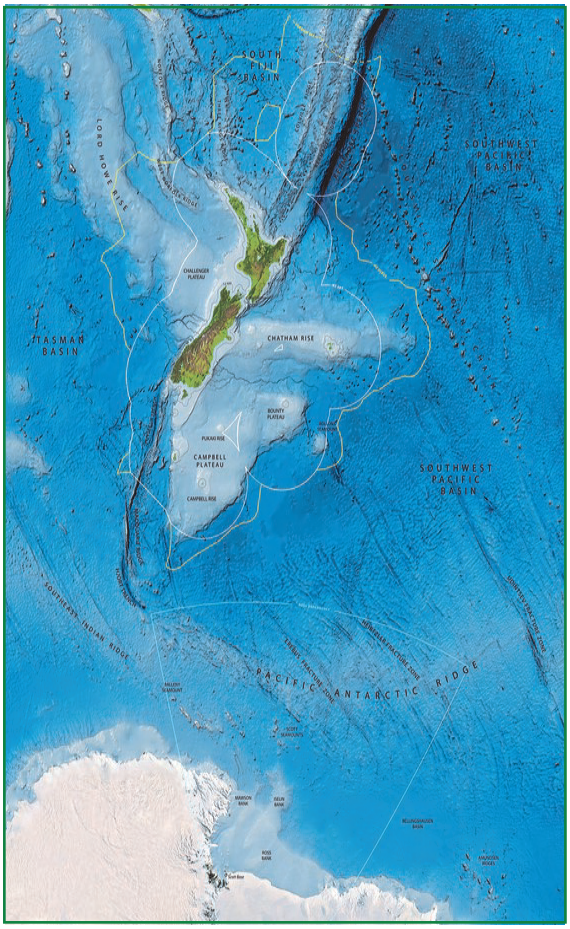
Protecting the territorial waters

Countries that border the sea have territorial waters. A very long time ago, this distance was 3 nautical miles (about 5.5 km) – the range of a cannon shot! In more modern times, the distance was 12 nautical miles (nmi) until 1982 when the United Nations established an international framework to create exclusive economic zones (EEZ) that stretch 200 nmi from the coastline.
To protect the territorial water a special system should be used in order to be able to first identify the dark vessel and then be able to locate them. In order to be able to do that we need three systems:

* Radar
* Direction Finder with the control station.
* Automatic Identification System Transponder.

Synthetic aperture radar (SAR)

instruments on board are very essential in determining the presence of dark vessels. SAR emits radar waves that strike the steel surface of a vessel and then ping back. SAR has real advantages over optical imagery (photos) – it isn't blocked by clouds and it does not require someone to be able to see a vessel amongst the camouflaged background of the waves.
The solution includes also an automatic localization system of the radio signals on the emergency channel, an aiding system for the search area and search paths calculation and a coordination console that assists the Coast Guard operator during SAR phases by visualizing search paths and the last known position of the vessel in distress.



Localization

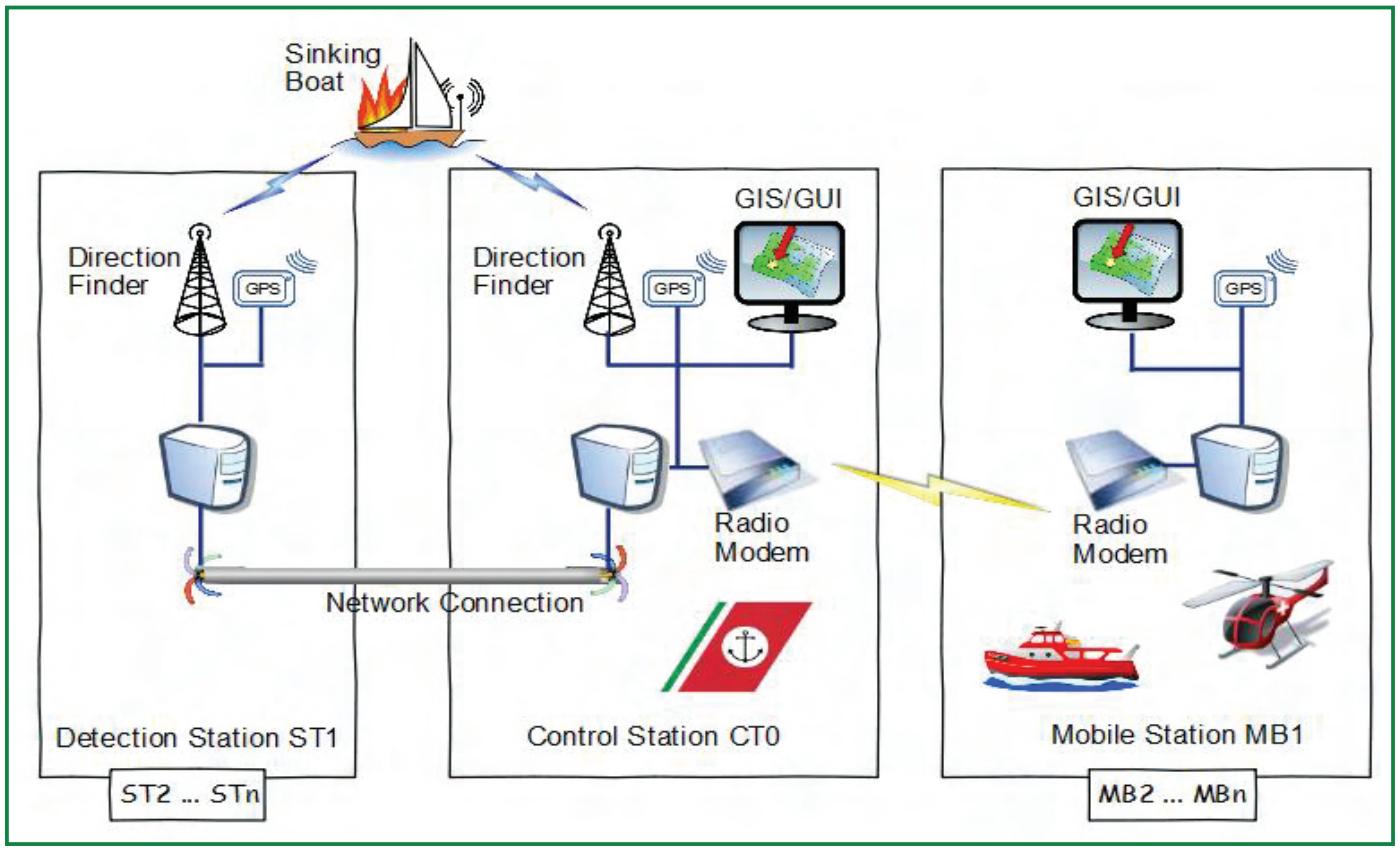
An intelligent system could detect and localize the vessel in the sea by monitoring the radio channel activity. Radio communications often occur so that an intelligent observer which looks from different locations could localize the vessel by signal direction detection. To this aim a radio direction finder (RDF), that is a device for finding the direction of an incoming radio signal, may be a useful tool. The Radio Direction Finder checks the signal strength of a directional antenna pointing in different directions. While old devices used a simple rotating antenna linked to a degree indicator, new devices use a dipole antenna to detect the signal.

In the past the RDF was used during the war to detect and identify secret transmitters in large region. The same idea can be applied to the different scenario of marine case. A group of RDFs controlled by an intelligent system can detect a distress signal and localize the source before that a communication between human beings even starts. The system we developed, is also able to track vessel movements after its first dentification (tracking feature). The detection range can be increased by the installation of new units along the coast. The intelligent system is composed by a society of intelligent agents which collaborate in monitoring radio frequencies, in matching the detections, in notifying every request. The system normally listens to the maritime radio emergency channels and whenever a signal is detected, a search of possible matches is looked for. When a match is found, the agents notify the discovery to other agents responsible for other system and to the Coast Guard personnel. When the source of the signal (the vessel) and the two detection stations are not aligned, a geometric triangulation gives the vessel position. The triangulation is computed between the direction vectors detected by the two stations. Of course, two vectors are necessary and sufficient but other ones may be used to improve the precision of the localization. Precision is in fact limited by the small error on the identification of the observed signal direction. The degree error becomes an estimated position error that is proportional to the distance between the source and the detection stations. In Figure 1 we show the simplest scenario where a dark vessel sends a signal that is in turn detected by a couple of coast stations. After the detections, the intelligent agents share that information and localize the source of the signal. In figure 1 we show the two vectors and the two angles used for triangulation. In the system there are two different kinds of stations:

Detection stations are unmanned and the only host hardware and software devoted to receive the radio signal and identify its direction. Control stations are manned and they host a complete hardware-software system thus including the capability of receiving informal ion from detection stations, performing triangulation and supporting SAR operations as described in the next subsection. Usually there is one control station responsible for each sea area according to Coast Guard procedures. Each detection station sends the following data to the control station:

* the radio channel of the signals obtained from detection finder
* the direction of the signal
* the position of the station

The time of detection the position and the time of detections are very useful to match detections from several stations. Of course, two detections of the same signal have a very similar detection time. The detections should be stored in an archive to solve problems about communication delays. In order to match a signal, the system searches a very similar detection from another station occurred in a fixed time window; the match with highest score is selected and used to compute the triangulation. So far, the computed localizations are sent to a GUI-GIS platform which shows a map to support the detection and finding of the dark vessel. The operator can update the data about any vessel shown by Fig. 1.



info@dicond7g.ng info@d7g.com www.d7g.ng
+234 80 3333 5533 +234 906 552 7916
NO 26 ALI AMODU CRESCENT, ASOKORO, FCT ABUJA