What we do

Digital Intelligence Services

1. Location Intelligence

In today's world, billions of devices are connected to the Internet; this connectivity generates vast volumes of data from various applications including metadata, GPS information, I.P Addresses and much more. Location intelligence in law enforcement involves analyzing geographic data to identify, predict, investigate and prevent crime patterns and hotspots.

2. LBS (Location Based Services)

* The Active solution can instantly locate specific targets (up to 50). However, this solution can only pinpoint the location of specific targets and has an accuracy range of 100-200 meters.

* The Passive solution. It allows for obtaining the geolocation of all subscribers in the network with an accuracy range of 25-200 meters.

3. Open-Source Intelligence (OSINT)

* In law enforcement, Passive OSINT allows law enforcement agencies to monitor social media, online forums, and other digital platforms to track criminal behavior, gather evidence, identify patterns of criminal activity, enhance investigations, support case development and ultimately improve their ability to combat crime and protect communities.

* In Politics, Active OSINT empowers politicians to influence public opinion through direct engagement By actively participating in online discussions and media interactions to shape perceptions, clarify issues, and build credibility, ultimately affecting public opinion on various topics and change trends from negative to positive and vice versa.

4. CCTV AI Module

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

5. Secure Messenger

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

6. Digital Forensics

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

7. Surveillance & Counter-Surveillance

Detect or implant audio & video Bugs, protect against adversaries' monitoring, safeguarding classified information and operations.

Products Overview

Digital Intelligence

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.

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?

> Investigate

> Monitor

> Protect

> Predict & Prevent

Detecting & Combating most types of crime

DICON D7G

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

Sustaining Global Defence Productions

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

- Global Visibility
- Correlation with multiple data sources
- Offline System
- Friendly graphical user interface.
- Giving the investigator the ability to achieve technical tasks.
- Navigating in time.
- Control access to information

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

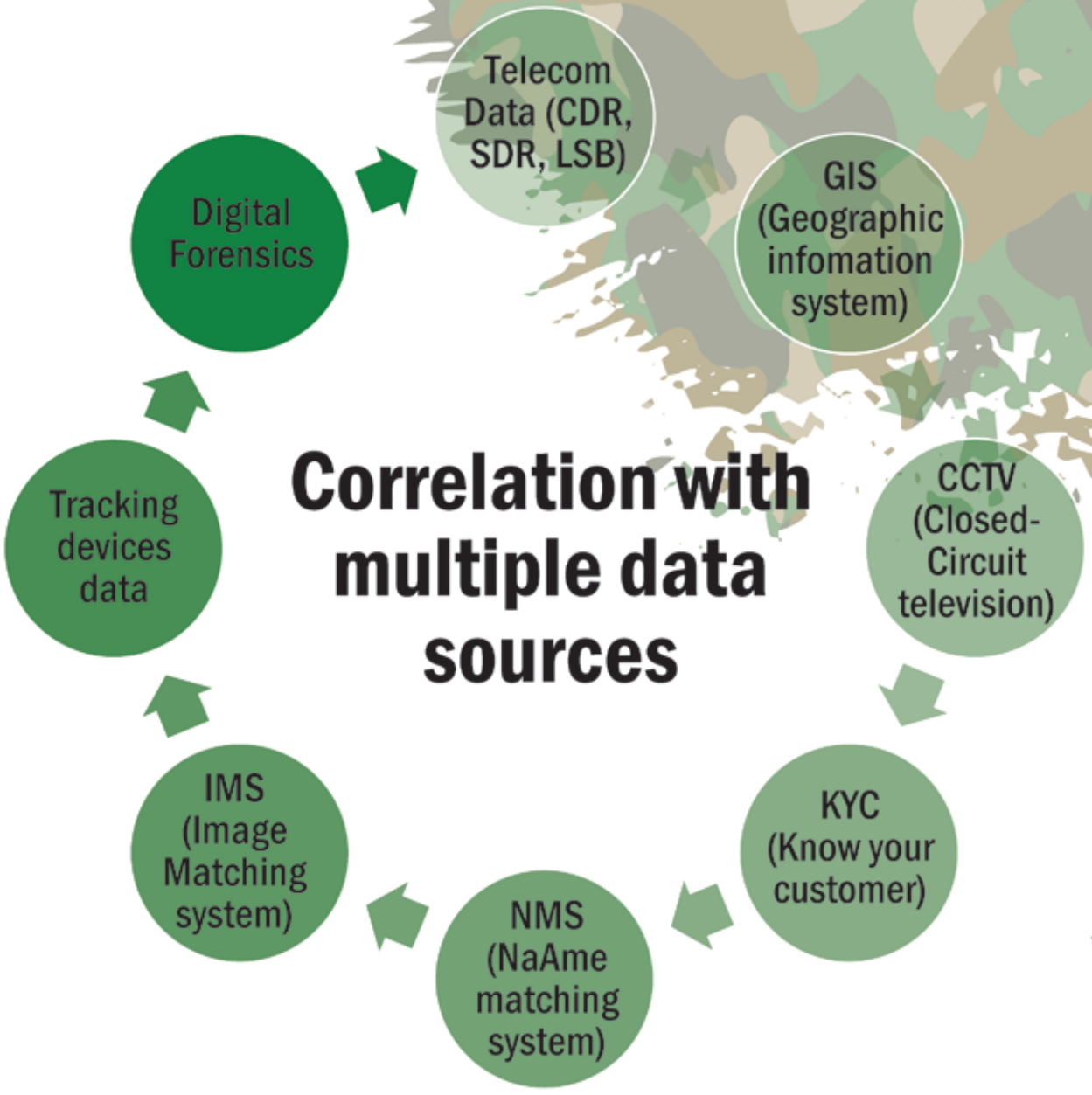
Handling	Handling structured and unstructured types of data
Ingesting	Ingesting the large amount of data in a measurable time
Executing	Executing any query or scenario in matter of seconds
Performing	Performing complex predefined scenarios in the background
	Flagging suspicious devices or entities
Providing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

Navigating in time: Backward & forward investigations

Understanding	Understanding the past
Analyzing	Analyzing the present
Predicting	Predicting the future

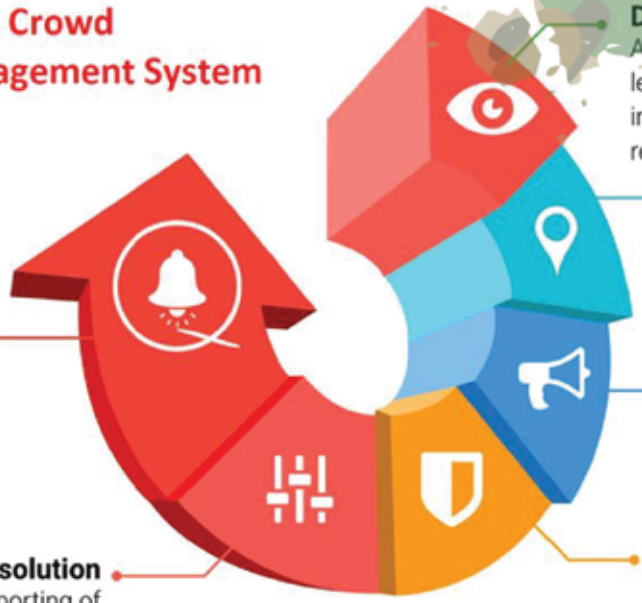
Control access to information

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



DICON D7G Alert management

Data Crowd
Alerts Management System



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

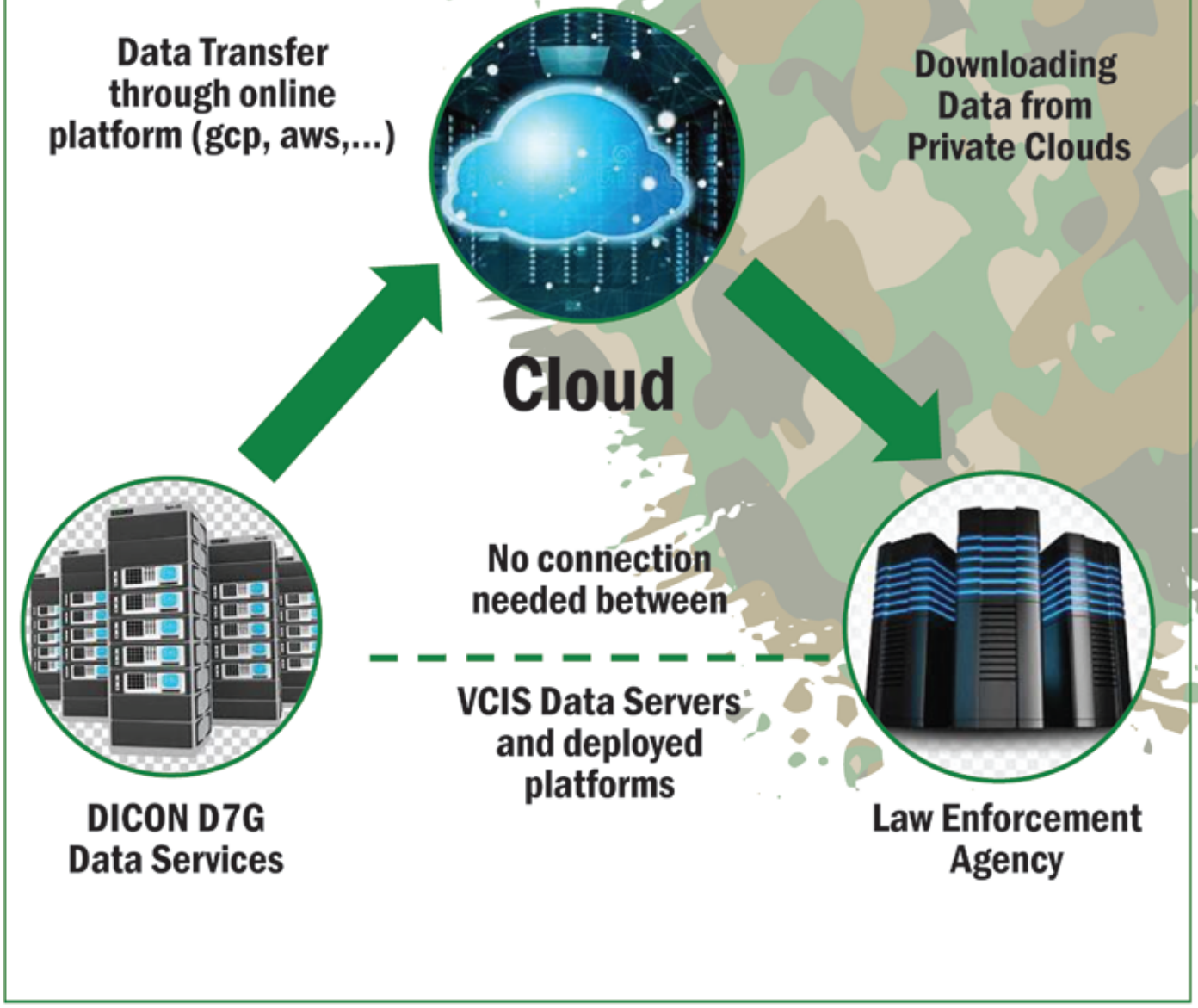
LOCATE - Analysis & Propagation
Analyzes data collected by human or AI technologies and shared with appropriate devices and resources

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

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

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


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

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.

3 Load Efficiency

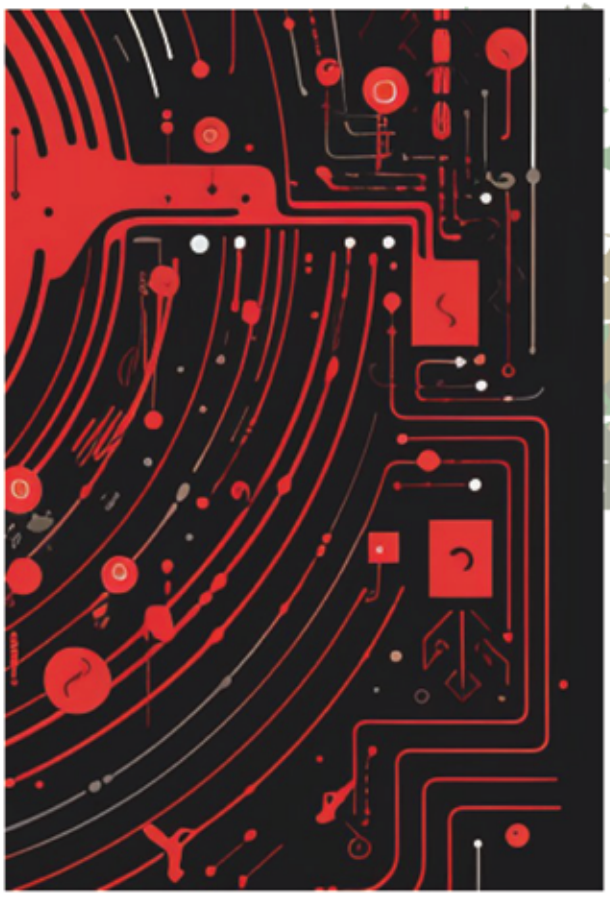
Our product excels in efficiently processing vast data volumes, ensuring swift and accurate insights for optimal decision-making.

Sustaining Global Defence Productions

OSINT Open-Source Intelligence

Intelligence-Driven Decisions

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



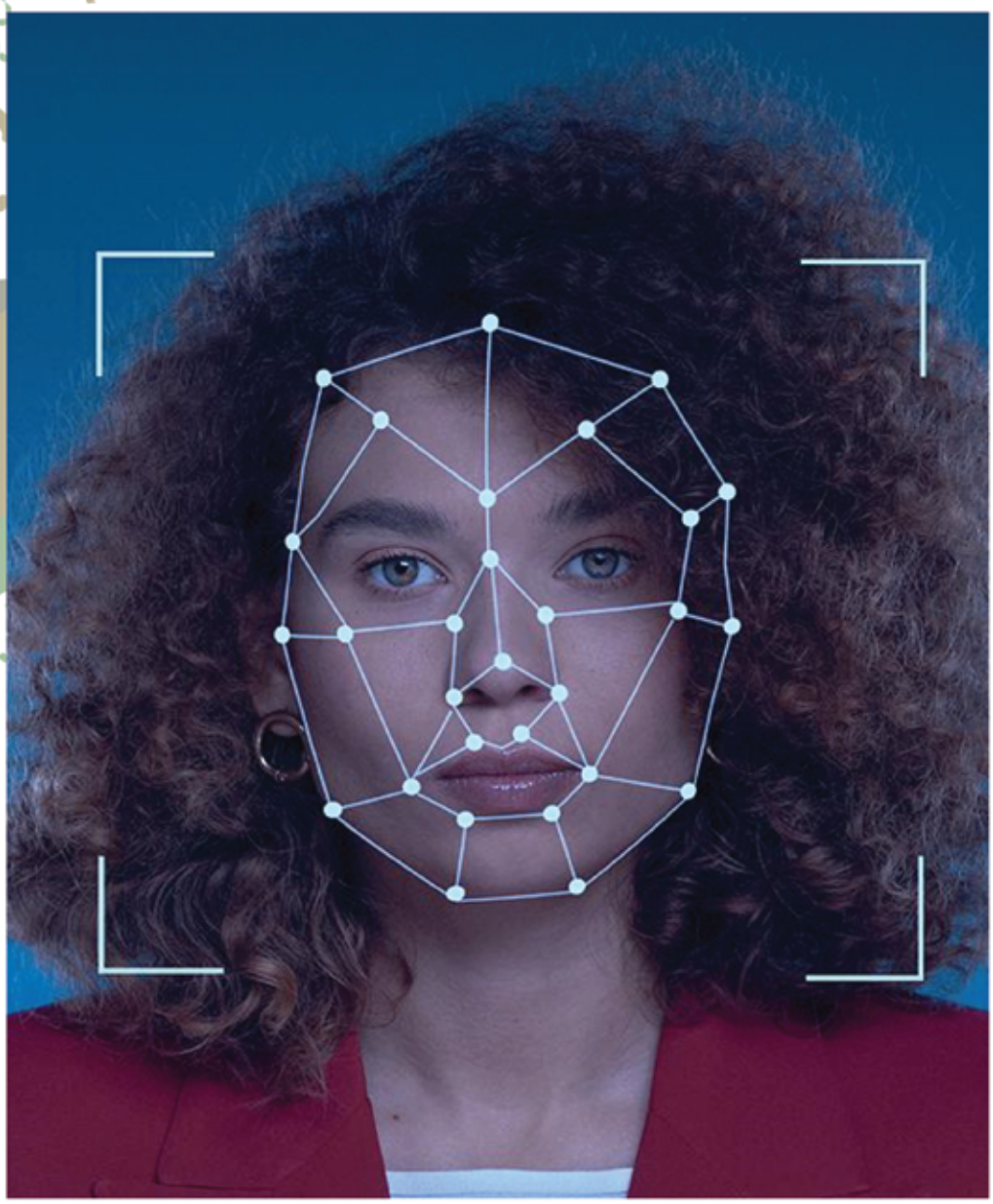
Analyze Large Sets of Data

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.

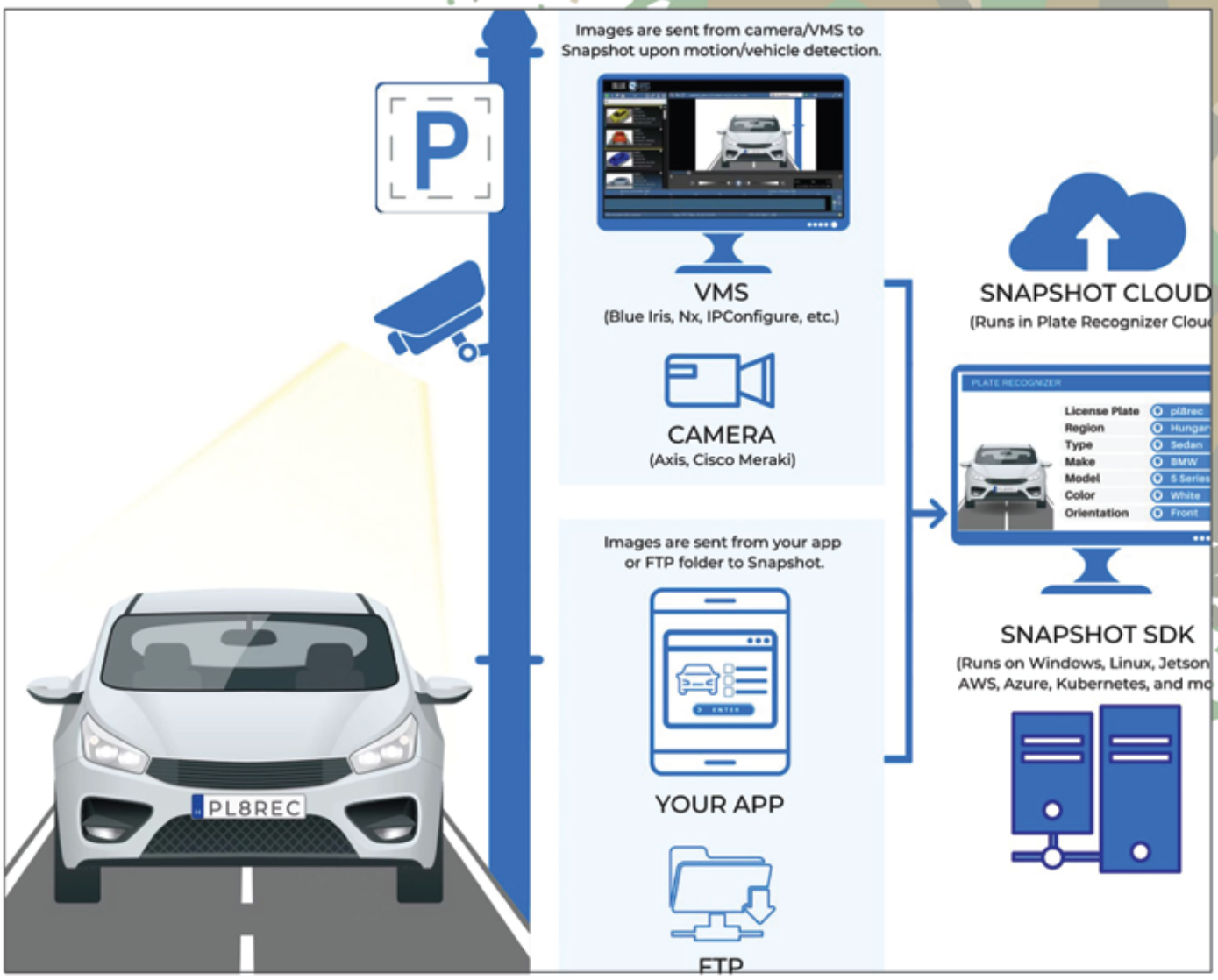
CCTV AI Engine

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%

You 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%

You 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.

Digital Forensics

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

Digital Forensics

Cloud Forensics

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

Vehicle Forensics

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

Digital Forensics

CCTV Forensics

- Extract videos from DVR, NVR, ...
- Recover deleted recordings
- Crime investigation
- Time consuming
- Preserve Evidence
- Bypass locked devices
- Supports various types of Video Recorders

Data Recovery

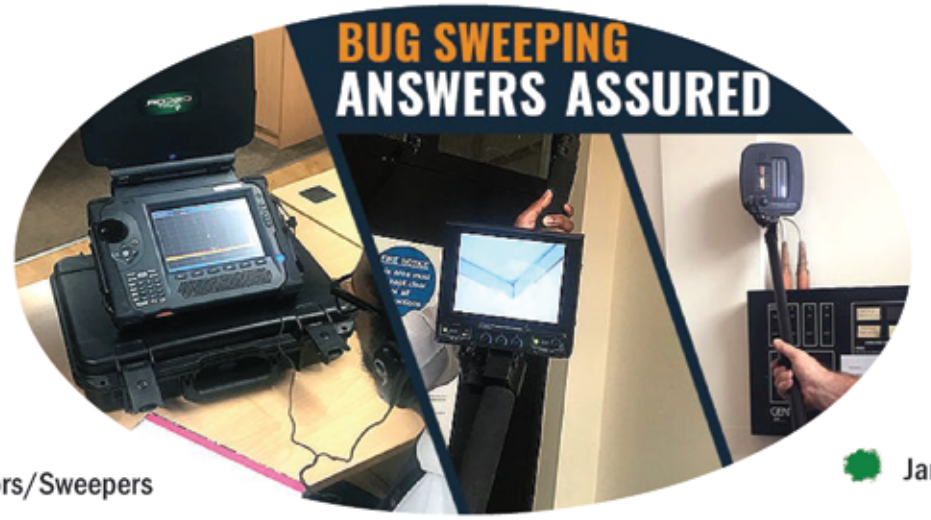
- Recover Deleted files
- Repair Damaged Hard Drives, SSD, USB,...
- Preserve Evidence
- Crime investigation

Digital Forensics

Technical Surveillance

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

Counter-Surveillance



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

Security information and event management

SIEM

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

Why SIEM Matters

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-incident investigations.

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

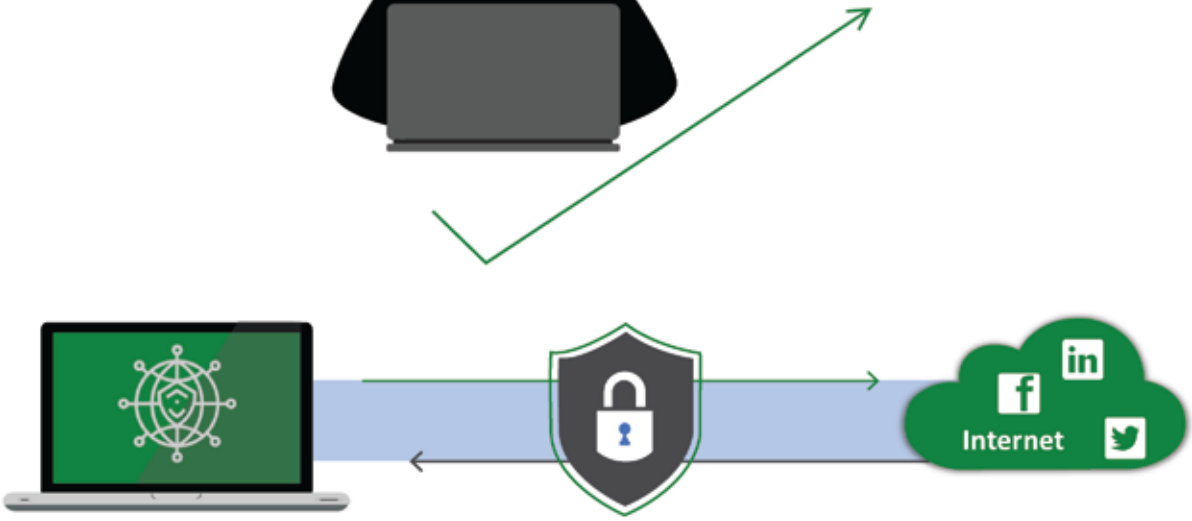
* Maintains an updated inventory of all endpoint devices, providing a comprehensive view of the organization's attack surface.

* 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

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.

Test Your Resilience

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.

Penetration Testing

Security Operation Center

SOC Services

58%

Skill Shortage

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

21%

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.

V C I S O

Cybersecurity Leadership Unleashed.

Virtual CISO

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

Sustaining Global Defence Productions

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.

Marine smuggling and dark vessels

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

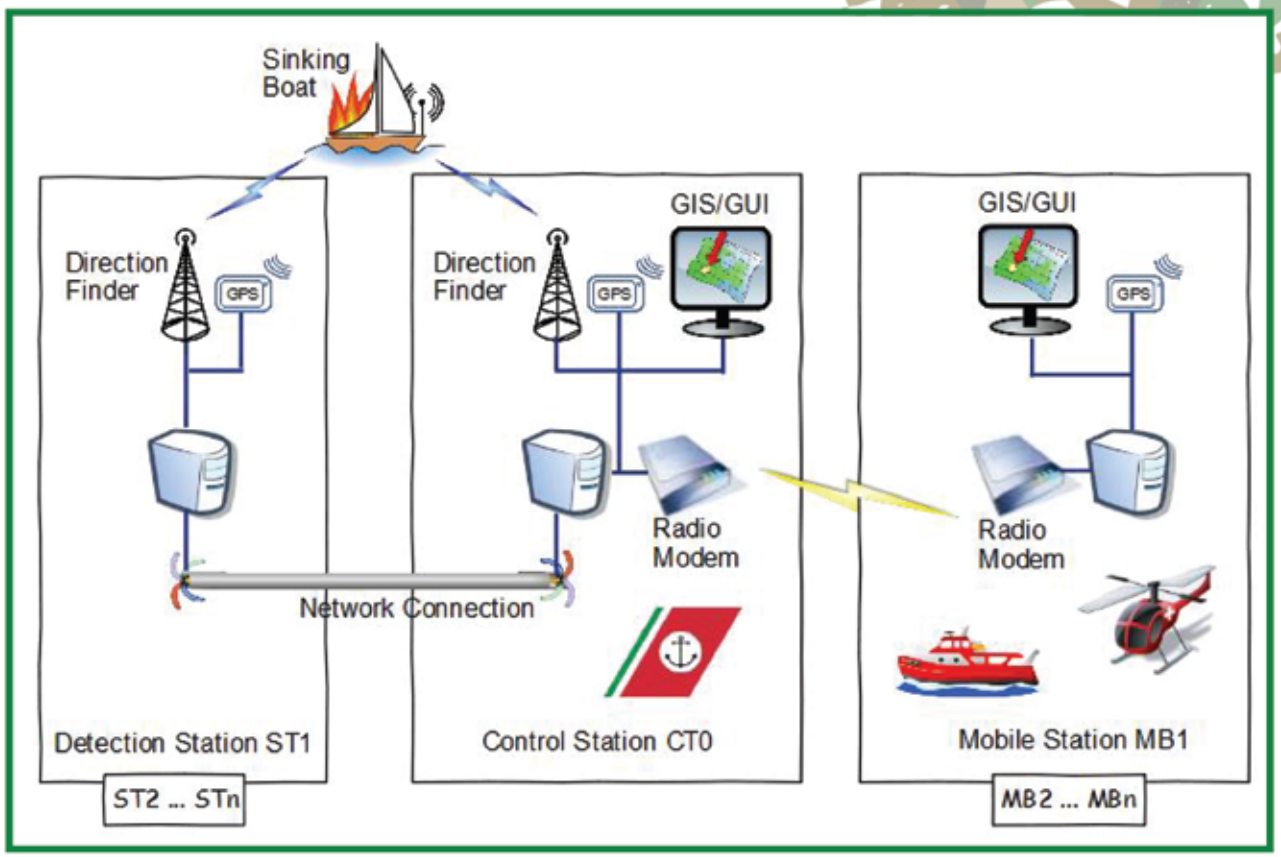
responsible for other system and to the Coast Guard personnel. When the source of the signal (the vessel) and the two detection stations are not aligned, a geometric triangulation gives the vessel position. The triangulation is computed between the direction vectors detected by the two stations. Of course, 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.



Sustaining Global Defence Productions

Army training

Localization

To safeguard our nation and its interests by employing cutting-edge technology, strategic planning, and the dedication of our personnel. We envision a future where our citizens and allies can thrive in a secure and stable environment, free from threats to their safety and sovereignty. Our agency will be at the forefront of innovation,

Developing and implementing strategies to counter terrorist threats, including domestic and international terrorism.

Developing comprehensive security strategies and plans to address potential threats and vulnerabilities. This includes risk assessments, scenario planning, and resource allocation.

Our Services

Providing professional security services worldwide.

Security devices Equipements

various types of security equipment and devices designed to protect people, property, and assets from threats, theft, vandalism, and unauthorized access.

Private military contractors

Alfa provides expert bodyguard protection. Our agents are well-trained and attentive.

Cyber Security

The protection of internet-connected systems such as hardware, software and data from cyberthreats.

Expertise in tactical training

This type of training is designed to equip security personnel with the knowledge, skills, and mindset required to effectively respond to a wide range of security threats and situations.

Travelling Bodyguards

High-profile individuals must take extra care and precaution during their travels.

Employee Screening

Help your company work smoother with safety regulations & stay safe.

Selling Tactical equipments for law enforcement

Tactical Supply Solutions is proud to be a partner in the vital work of our nation's law enforcement agencies. We work tirelessly to provide the tools and equipment needed for those who put their lives on the line daily to protect our communities.
Our dedication to quality, reliability, and innovation is unwavering, ensuring that our clients are equipped to face any challenge they encounter in the line of duty.

Security Services solutions & consultancy

Alfa Defense promises superior security solutions in what the industry requires.

Sustaining Global Defence Productions