KABADI

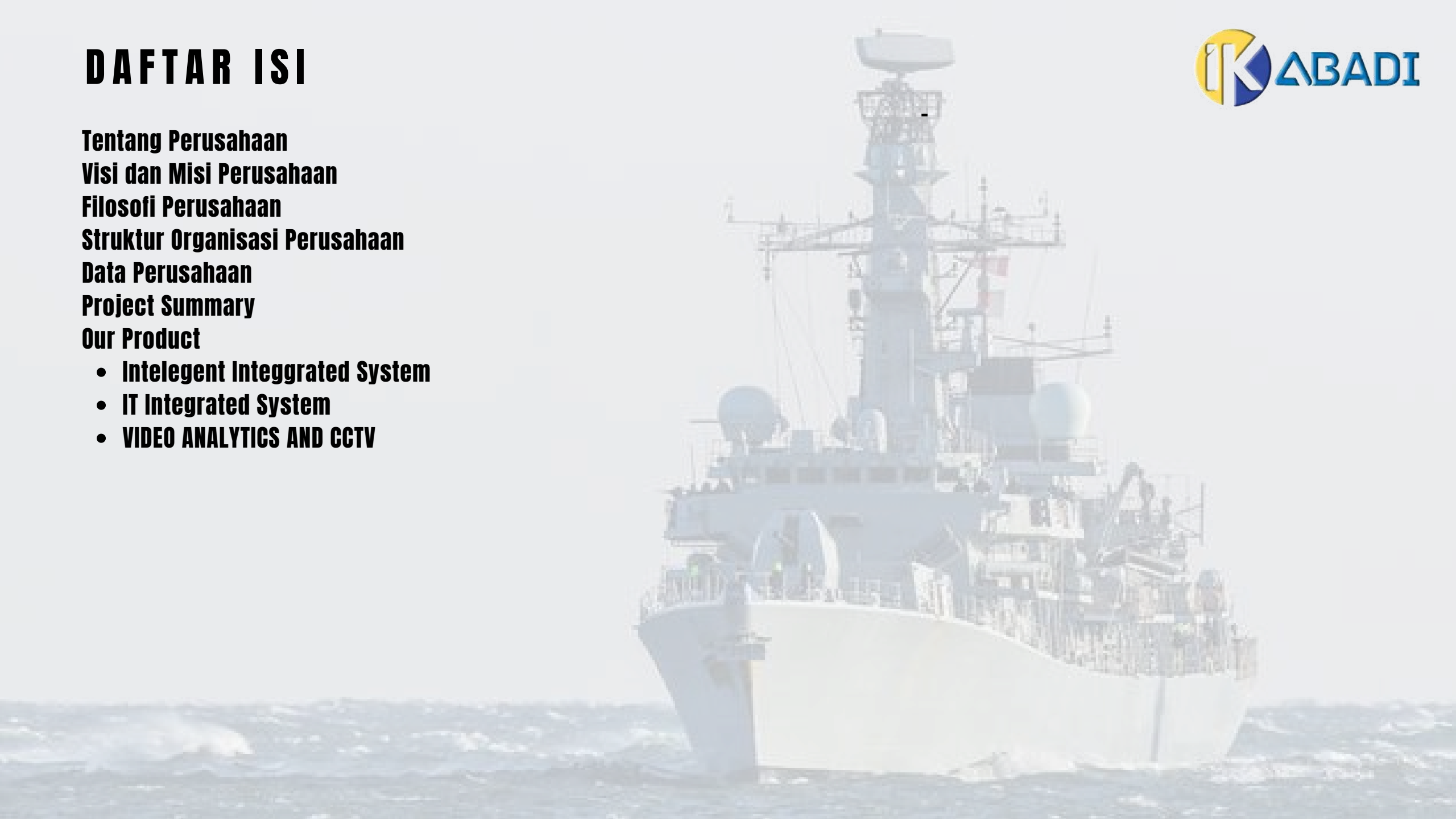
COMPANY PROFILE

PROFESIONAL, KUALITAS,
KEAMANAN, DAN KEPERCAYAAN

DAFTAR ISI

Tentang Perusahaan
Visi dan Misi Perusahaan
Filosofi Perusahaan
Struktur Organisasi Perusahaan
Data Perusahaan
Project Summary
Our Product

- Intelegent Integgrated System
- IT Integrated System
- VIDEO ANALYTICS AND CCTV



TENTANG PERUSAHAAN

Kami adalah perusahaan yang bergerak di bidang pertahanan dengan tenaga ahli yang profesional dan berpengalaman dalam menciptakan berbagai produk di bidang pertahanan untuk pemerintahan, militer, organisasi intelijen dan kepolisian. Kami berkomitmen memberikan pelayanan prima dengan solusi terbaik.

VISI & MISI PERUSAHAAN

MISI

Menjadi perusahaan yang kredibel, amanah dan terbuka dalam memberikan pelayanan yang profesional, ramah.

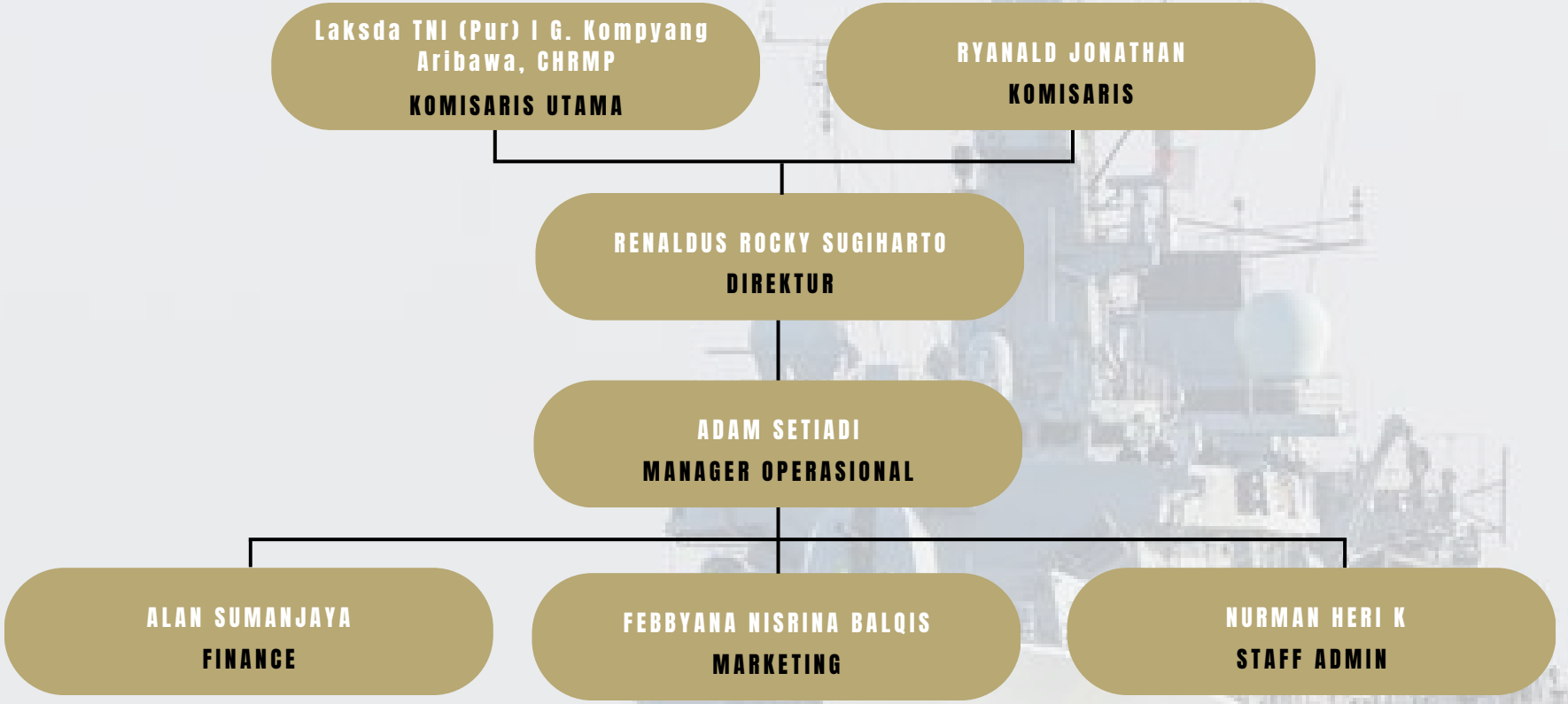
VISI

Menciptakan lingkungan kerja yang kondusif dan komprehensif, membangun sumber daya manusia yang berintegritas dan profesional serta memenuhi kebutuhan pengguna dengan standar mutu dan mengembangkan sistem informasi modern

FILOSOFI

“Menjadi Perusahaan Jasa Pengadaan Barang Terbaik, Terpercaya dan Bangga bagi Bangsa Indonesia serta diakui Dunia”

STRUKTUR ORGANISASI
PT. INTI KASIH ABADI



DATA PERUSAHAAN

Deed of company
Deed of Establishment No. 15 July 10, 2023

Business Registration Number
No : 1307230033965

List of Registered Companies Kemenkumham
No : AHU-0050110.AH.01.01 YEAR 2023
DATE 11 JulY 2023

PROJECT SUMMARY

IT DEVELOPMENT PROGRAM

INDONESIA NAVY (ARMADA RI)

OUR PRODUCT

IT INTEGRATED SYSTEM

SATU DATA ARMADA NUSANTARA

SATU DATA ARMADA NUSANTARA (SDAN) ADALAH BAGIAN PROGRAM INTEGRATED WARSHIP INFORMATION SYSTEM (IWIS) YANG MERUPAKAN IMPLEMENTASI DARI NETWORK CENTRIC WARFARE (NCW). DENGAN MELAKSANAKAN DIGITALISASI DAN INTEGRASI DATA UNTUK MEWUJUDKAN SATU DATA TNI AL PADA SISTEM SENJATA ARMADA TERPADU (SSAT) DALAM RANGKA PENGAMBILAN KEPUTUSAN YANG LEBIH CEPAT, TEPAT DAN AKURAT SERTA TERJAMIN KEAMANANNYA.

DASAR

GRAND DESIGN NETWORK CENTRIC WARFARE (NCW)	KEPUTUSAN KASAL NomorKEP/1709/VII/2024, Tanggal12 Juli2024 TentangGrand Design NCW TNI AL
SATU DATA TNI AL	PERKASAL NOMOR 36 TAHUN 2023, Tanggal1 Agustus2023 TentangSatu Data Tentara Nasional Indonesia Angkatan Laut
KAJIAN IWIS TNI ANGKATAN LAUT	Surat KadisinfolahtalKe AskomlekKasalNo B/1433/X/2024 Tanggal29 oktober2024 tentangKajian Integrated Warship Information System (IWIS)
KAJIAN SATU DATA ARMADA NUSANTARA	Surat PangkoarmadaRI NOMOR B/940/VII/2024 Tanggal30 Juli2024 Kajian TentangDigitalisasiSatu Data Armada Nusantara

LATAR BELAKANG

KONDISI SAAT INI

- Belum terdigitalisasi seluruh unsur SSAT
- StandarData yang berbedadi seluruhinstansi
- KeterbatasanInfrastrukturteknologidi Armada beserta jajarannya
- KurangnyaSistemMonitoring armada secara terpusat
- Keterbatasan Keamanan dan Kerahasiaan data
- BanyaknyaKRI yang perludimonitoruntuk kesiapan nya

TUJUAN

1. **Digitalisasi dan Integrasi Data SSAT**: Memudahkan akses data dan mendukung pengambilan keputusan yang lebih tepat berdasarkan data yang terintegrasi.
2. **Standarisasi Data Antar-Instansi**: Mengurangi kesalahan interpretasi, memudahkan kolaborasi, dan mempercepat analisis serta pelaporan.
3. **Peningkatan Infrastruktur Teknologi di Armada**: Memperkuat konektivitas dan akses data, mendukung operasional yang lebih efektif.
4. **Sistem Monitoring Armada Terpusat**: Memungkinkan pemantauan real-time kondisi dan pergerakan armada, meningkatkan respons dan keamanan.
5. **Perwujudan Network Centric Warfare**: Meningkatkan komunikasi dan koordinasi antar Unit, mendukung strategi dan taktik untuk menghadapi ancaman dengan menguasai informasi dalam jaringan terpusat
6. **Pengambilan Kebijakan yang Lebih Cepat, Tepat DAN AKURAT Berdasarkan Data**: Mendukung efisiensi operasional dengankeputusan berbasis data yang valid.
7. **Keamanan Data yang Terjamin**: Melindungi data sensitif dari ancaman siber, menjaga kerahasiaan dan integritas informasi.

AD-AI

Advertisement Intelligence

AD-AI IS A STRATEGIC TOOL, UNCOVERING THE PRECISE DETAILS OF WHAT UNFOLDS WITHIN A DESIGNATED AREA . IT OFFERS A DY NA MIC A LTERN ATIVE T O CONVENTIONAL TACTICAL INQUIRIES.

HARNESSES THE POWER OF BIG DATA TO COLLECT VAST QUANTITIES OF INFORMATION FROM EVERY SMART DEVICE WITHIN A SPECIFIC AREA OF INTEREST

AD-AI

THE CAPABILITIES

UNVEIL THE IDENTITIES OF INDIVIDUALS WITHIN A LOCATION AND ILLUMINATE THEIR ACTIVITIES – INCLUDING WHEN, WHERE, AND WITH WHOM – PROVIDING INVALUABLE INSIGHTS FOR STRATEGIC DECISION MAKING.

THE SYSTEM

BIG DATA
AD INTELLIGENCE

- Area based intelligence
- Massive data ingestion
- User behavior
- Apps on device

AD INTELLIGENCE
Understand movement patterns, user ac tivit y and impor tan t devic e parameters

- OS version
- Phone model
- Installed apps
- Network type
- Ip address
- Location
- Habits
- Demographics

UNCOVER
INTELLIGENCE
INVESTIGATION CLUES

- Top locations & Meeting points
- Movement patterns
- Behavior & habits
- Understand relationships
- Detect anomalies
- Set alerts based on activity

AD-AI

KEY ADVANTAGES

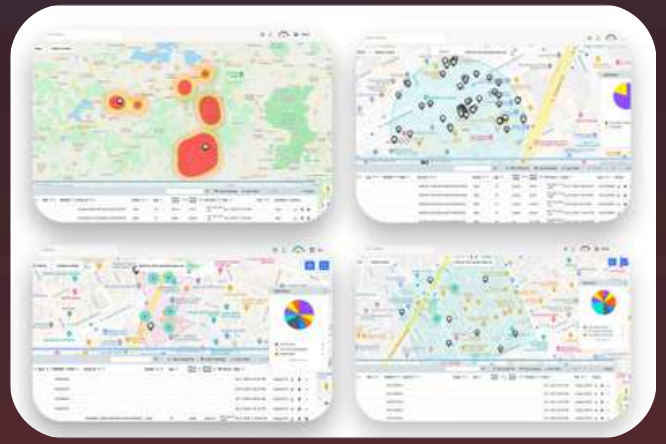
- Reveal real-time / Historical GPS location
- MSISDN to an AdID
- Monitor areas of interest
- Comprehensive insight reports
- Patterns behavior
- Incident analysis

AD-AI

OPERATIONAL PROCESS&WORKFLOW

TRIGGER AN INVESTIGATION FOCUSED ON A SPECIFIC AREA OF INTEREST, UNCOVERING THE ADIDS ASSOCIATED WITH DEVICES PRESENT AT ANY GIVEN MOMENT. CROSS-REFERENCING WITH LARGE DATABASES, REVEAL THE MSISDNS LINKED TO THESE DEVICES, DELIVERING CRITICAL INSIGHTS FOR FURTHER ANALYSIS AND ACTION.

AD-AI activated → Select an area of interest → Reveal real-time or historical GPS location → Investigate behavior relationships and activities



ATLAS GGS

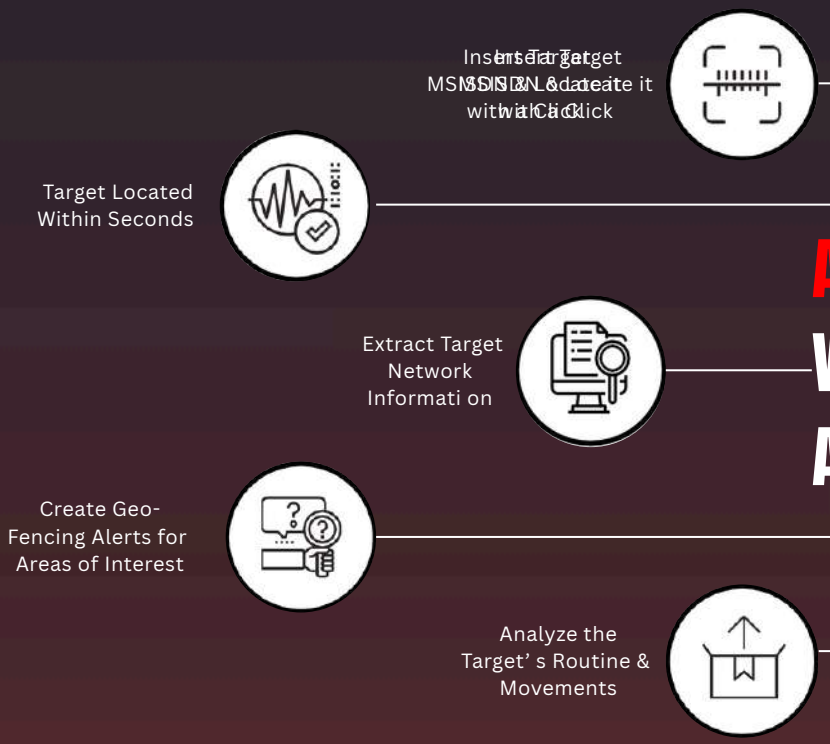
Global Geolocation System

A GLOBAL GEOLOCATION SYSTEM REMOTELY LOCATES TARGETS USING MAP-BASED INTELLIGENCE OVER 2G, 3G, 4G & 5G NETWORKS

ATLAS GGS BASED ON

The SS7 is a signaling system 7 for common channel signaling system used in international and local telephone networks

ATLAS GGS WORKFLOW AND ARCHITECTURE



ATLAS GGS
KEY OPERATIONAL FEATURES

- Out of the Box solution
- Centrally Controlled
- User Friendly
- Does not require any domain expertise
- Rapid Deployment
- Mobile and Adaptable

ATLAS GGS
ACTON
BUTTONS

Location finding

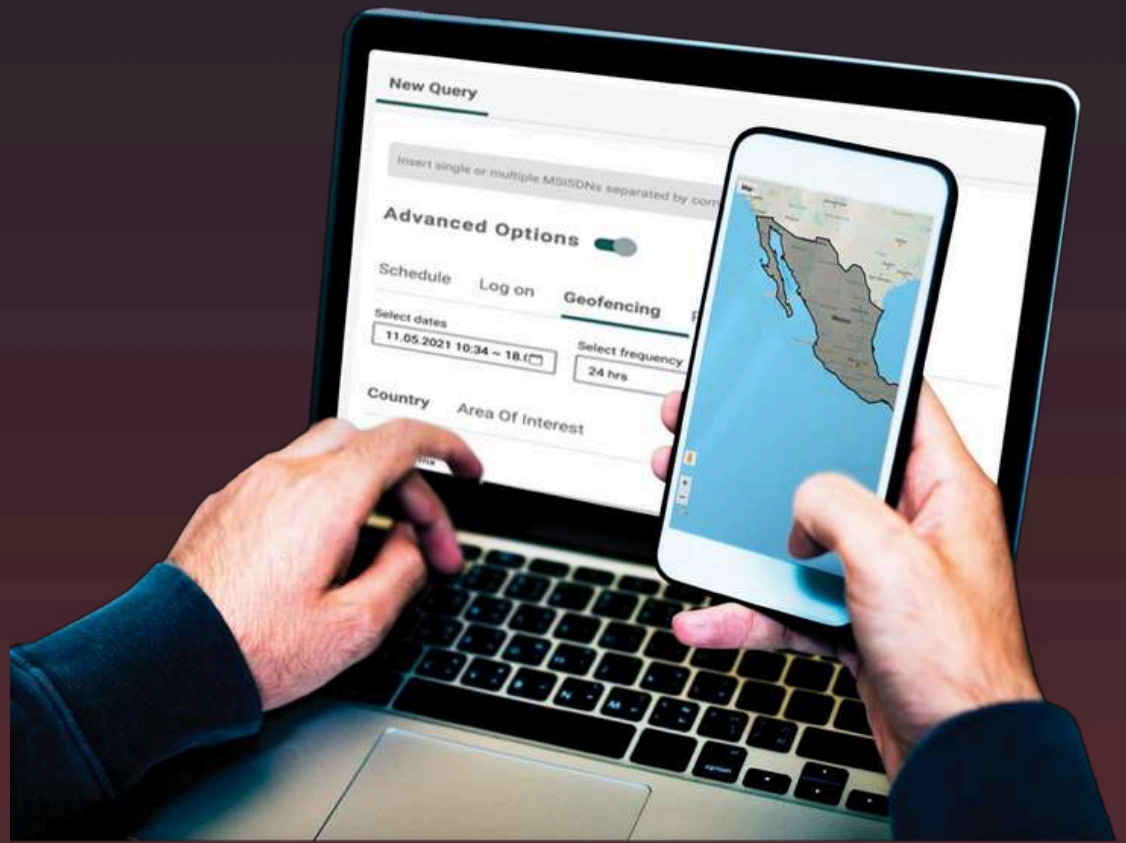
Geofencing

Neighbori ng Cells

ATLAS GGS
GEOFENCING

GEOFENCING NOTIFIES YOU WHEN A TARGET ENTERS OR LEAVES A SPECIFIC AREA:

- COUNTRY
- Area of Interest



ATLAS GGS
GEOLOCATION ANALYTICS

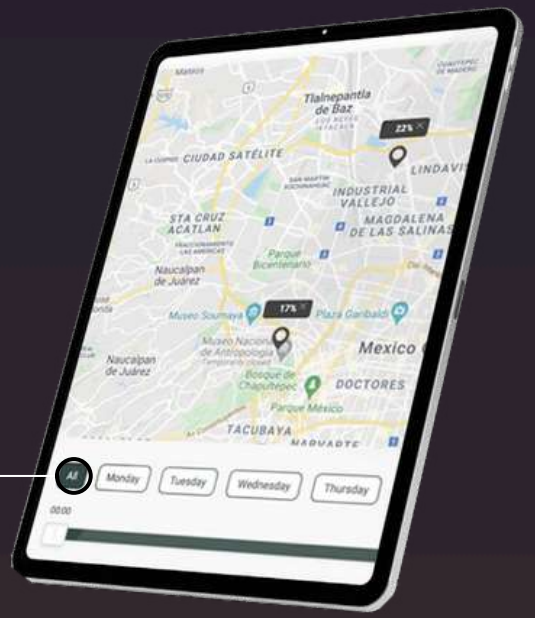
HEATMAP: Graphical representation of the historical positions of a target

TIMELINE: Shows all historical target location information as pins.

LAST SEEN: This shows the most recent target location information.

ATLAS GGS
PREDICTED LOCATIONS

Data analysis engine that predicts the probability of where the target will be at a future time defined by the user.



ATLAS GGS
INTELLIGENCE REPORT

ATLAS GGS
PLATFORMS

STATIONARY

MOBILE

CLOUD BASED

BTSSTRESSOR

BTS DENIAL OF SERVICE

The BTS Stressor offers an Active method for stressing cellular base stations across All technologies and frequencies. Utilizing Combined Methodologies, it induces simulations of Denial of Service (DOS), causing severe service disruptions and overloading the cellular infrastructure.

This sophisticated solution is engineered to challenge commercial cellular base stations (BTS) and IMSI Catchers, offering unparalleled capability in disrupting adversary communications.

BTSSTRESSOR

THE CAPABILITIES

The system employs a series of Combined Disruptions aimed at inducing either a complete overload of IMSI Catcher BTS / commercial cellular base stations or triggering a no-service mode for registered phones.

THE SYSTEM

SCAN

The entire cellular spectrum, covering 2G, 3G, 4G, 5G NSA & SA

DETECT

Analyze over 100 broadcast parameters to identify certain abnormalities in less than 10 seconds

ALERT

Automated alerts on suspicious cells

DOS

Stress the cell and cause a Denial Of Service

BTSSTRESSOR
KEY ADVANTAGES

- Comprehensive Spectrum Scanning
- Advanced Abnormality Analysis
- Real-Time Suspicious Activity Alert
- Robust Combined Stress Capabilities
- Manual / Automatic Operation
- Incident analysis

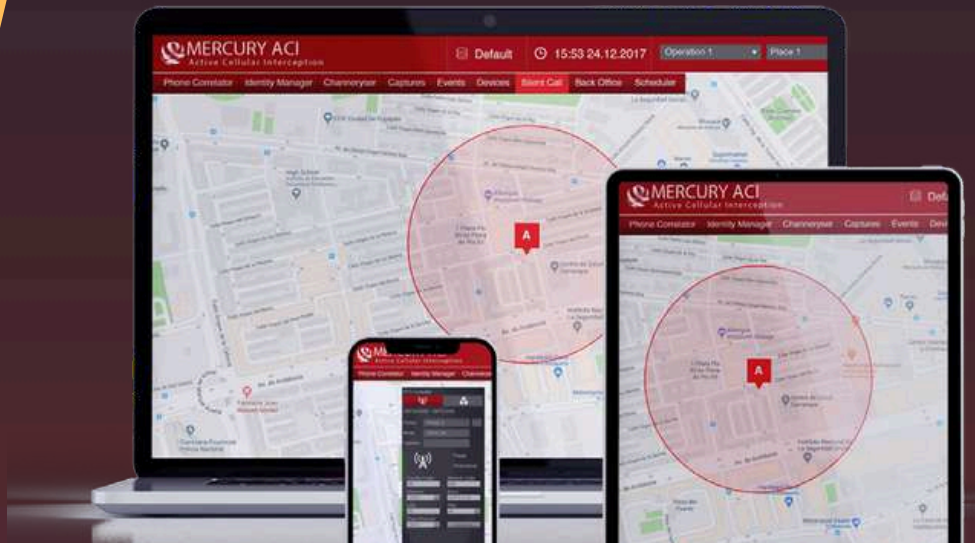
MERCURY ACI

Active Cellular Interception

AN ACTIVE CELLULAR INTERCEPTION (ACI) IS A TACTICAL SYSTEM THAT ACTIVELY INTERFERES IN COMMUNICATIONS BETWEEN CELL PHONES AND BASE STATIONS, ONCE INTERCEPTED, IT GAINS FULL CONTROL AND MANIPULATES IN MULTIPLE WAYS

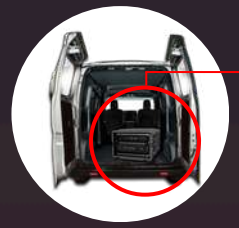
MERCURY ACI PRODUCTS FAMILY

A TACTICAL SYSTEM FOR INTERCEPTING TARGETED CELLPHONES. A COMPACT, DISCRETE AND POWERFUL PLATFORM THAT PLACES OPERATORS IN THE MIDDLE OF TARGET COMMUNICATIONS AND ENABLES PROACTIVE, COUNTERINTELLIGENCE OPERATIONS

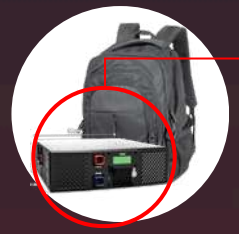


KEY OPERATIONAL FEATURES

COMPACT AND COVERT MOTORCYCLE MOUNTED SYSTEM



VEHICLE DEPLOYMENT



COMPACT AND COVERT BACKPACK TACTICAL SYSTEM

DUAL BTS DRONE TACTICAL SYSTEM

FAMILY PRODUCTS KEY OPERATIONAL F E A T U R E S

EXTRACT ID
Extracts the identity of the target

AREA JAMMING
Enables jamming of target's area

BLOCK
Blocks the target's calls and SMSs

MANIPULATE

FAKE CALLS
Fakes calls and SMSs from\ to the target

FAMILY PRODUCTS KEY OPERATIONAL F E A T U R E S

- Supports all Network protocols (GSM, UMTS, LTE)
- Enables listening and recording of Voice calls
- Intercepts SMS Messages
- Operates with all service Providers
- Locates the Direction of the Target
- Highly Portable

FAMILY PRODUCTS KEY OPERATIONAL ADVANTAGES

- Light weight and compactible (small dimensions)
- Internal 60W Power amplifier
- Remotely controlling the system from a phone app
- Wi-Fi connection
- Can be operated from a tablet
- Various deployment options: backpack- car- motorcycle- drone
- 4G silent call with internal TDD in the box
- Only two hidden antennas
- Easy deployment

NYX DETECTOR

FAKE CELL DETECTOR

The NYX DETECTOR detects the use of IMSI Catchers and Active Interception Systems. Robust, with outstanding sensitivity, the platform is designed to provide 24/7 peripheral protection where deployed.

NYX DETECTOR

A TACTICAL SYSTEM
FOR THE DETECTION OF
IMSI CATCHER

NYX DETECTOR

OPERATIONAL WORKFLOW

Imports external databases of cellular networks/ BTS locations

Scans all BTS's in the area

Analyses all BTS parameters

Alerts about BTS anomalies

Alerts about fake BTSs (Active Interception Systems in the area)

Locate the fake BTS

KEY FEATURES

DETECTION

Once an active system has been found an alert is sent to the operator and all relevant personnel, and the location is presented.

ACCURACY

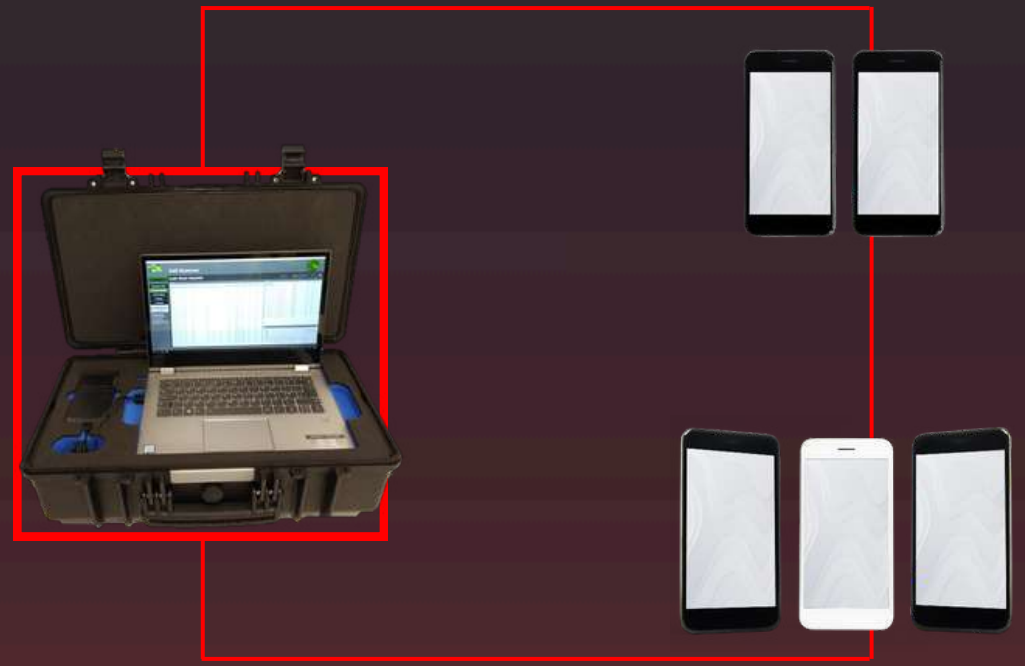
No false positives by using multiply verification parameters.

PROTECTION

The system is designed for 24/7 monitoring.

COVERT

The system is fully passive no transmission therefore it cannot be detected nor traced.

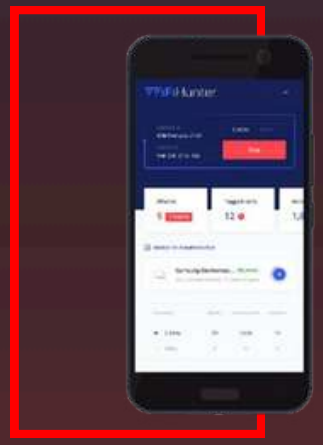


NYX DETECTOR UPGRADES

Wi-Fi intrusion detection support

NYX Detector can be upgraded to support WiFi intrusion detection, which can run alongside with the Fake cell detection.

The WiFi detector scan both 2Ghz and 5Ghz, detected real-time attacks such as KRACK, WPS & brute force, and locate its source. It can also disconnect specific clients from the network.



External directional finding unit

The external directional finding unit includes an additional scanning module and a directional antenna. The antenna helps identify the direction of the signal source, therefore improving the search effectiveness. The additional scanning unit allows scanning and searching at the same time.

SOTERIA

SECURITY SAFETY TECHNOLOGY

Soteria is a world leader in our field, pioneering innovative frontiers of intelligence since 2009 with tens of government installations worldwide. Soteria developed UGINE™, a unified system for data fusion research and investigation,a robust, full-cycle WEBINT environment featuring a realtime analytics platform with full web coverage.

Founded by intelligence agency professionals, Soteria is a privately held company that develops and markets cutting edge Intelligence Solutions and Platforms.

Customer satisfaction is at the heart of everything we do, and we pride ourselves on post-install support that is both efficient and useful.

THERE IS NO 'CATCHING UP' WITH INTELLIGENCE

Unify Your Data

With full-spectrum access to critical resources, UGINE™ creates a full intelligence picture from many different pieces. Empower analysts with the data they need.

The Intelligence Edge

UGINE™ fully integrates WEBINT tools, diving deep into data to empower organizations with continuously enriched awareness and accelerated intelligence.

Always Alert, Always Ready

Analysts and operators facing complex, large scenarios can focus on what counts with UGINE™ real-time situation awareness and rapid alerts.

Speed and Savings

UGINE™ 's small data footprint ensures critical resources are focused on collection, not collation. The highly efficient inverted index sidesteps database duplication and dramatically lowers overhead.

Gain a
UNIFIED VIEW
across sensors
and systems

Generate
PREDICTIVE
Insights

RESPOND PROACTIVELY
with the right
operational profile

Achieve Effective
SITUATIONAL AWARENESS

Access
VITAL INFORMATION
in real time

UGINE™ uses a powerful integration engine to enrich and enhance the power of data streams, on demand. Fuse your existing sensors and sources to innovative web and social media analytics.

Adaptive Solution

UGINE™ seamlessly connect to all your data repositories providing immediate value from cross-system data fusion. With auto data mapping and self-data-discovery, connecting a new source is a simple task – not a multi-month expert project. Furthermore, the UGINE™ Adaptive Data Model (ADM) can fit into your organization's "modus operandi" shortening the traditional learning curve of a new system from months to days.

Hybrid Index

The UGINE™ engine is built on a hybrid index – best suitable for handling both structured and unstructured data efficiently and effectively, with minimum data duplication and without overloading the source systems.

Data Sense-making

UGINE™ combines Natural Language Processing (NLP) and a semantic engine for big data sense-making. By correlating extracted Entities, Topics and Relations with data patterns and major events, UGINE™ provides much greater insight into risks and investigation with actionable recommendation.

Customizable Dashboards

UGINE™ comes with a comprehensive set of dashboards, administrator and user reports that can be easily modified, customized and extended to provide the highest productivity and user experience.

WINTERIA

WEB INTELLIGENCE SYSTEM

Developed by intelligence specialists, WINTERIA is a holistic, fully integrated, Web Intelligence platform designed for comprehensive intelligence gathering and investigation management. WINTERIA dives into the ocean of data available in open, as well as covert sources, throughout the various online and darknet platforms.

WINTERIA provides multilingual and multisource collection and analysis capabilities, as well prompt alerting and advanced reporting capabilities, aimed at
enhancing and leveraging the intelligence collection and investigation workflow.

WINTERIA offers a full-suite intelligence solution, including advanced features and capabilities

PROFILER

Aimed at rapid background profiling of targets, WINTERIA Profiler executes prompt and complex search throughout the various social media and mobile platforms, uncovering targets' online as well as offline presence. Therefore, the collected data is enriched by the system, providing full overview of the target entity.

WIDE SEARCH & Case Management

Throughout advanced and distinctive methods, WINTERIA Wide Search module is designed to execute multi-layered complex intelligence gathering, covering websites, social media platforms, darknet hidden services, Telegram groups and mobile platforms. Moreover, all data is indexed within the system, and advanced analytical insights are established and generated for each investigation, uncovering potential leads and further pivots.

WIDE SEARCH & Case Management

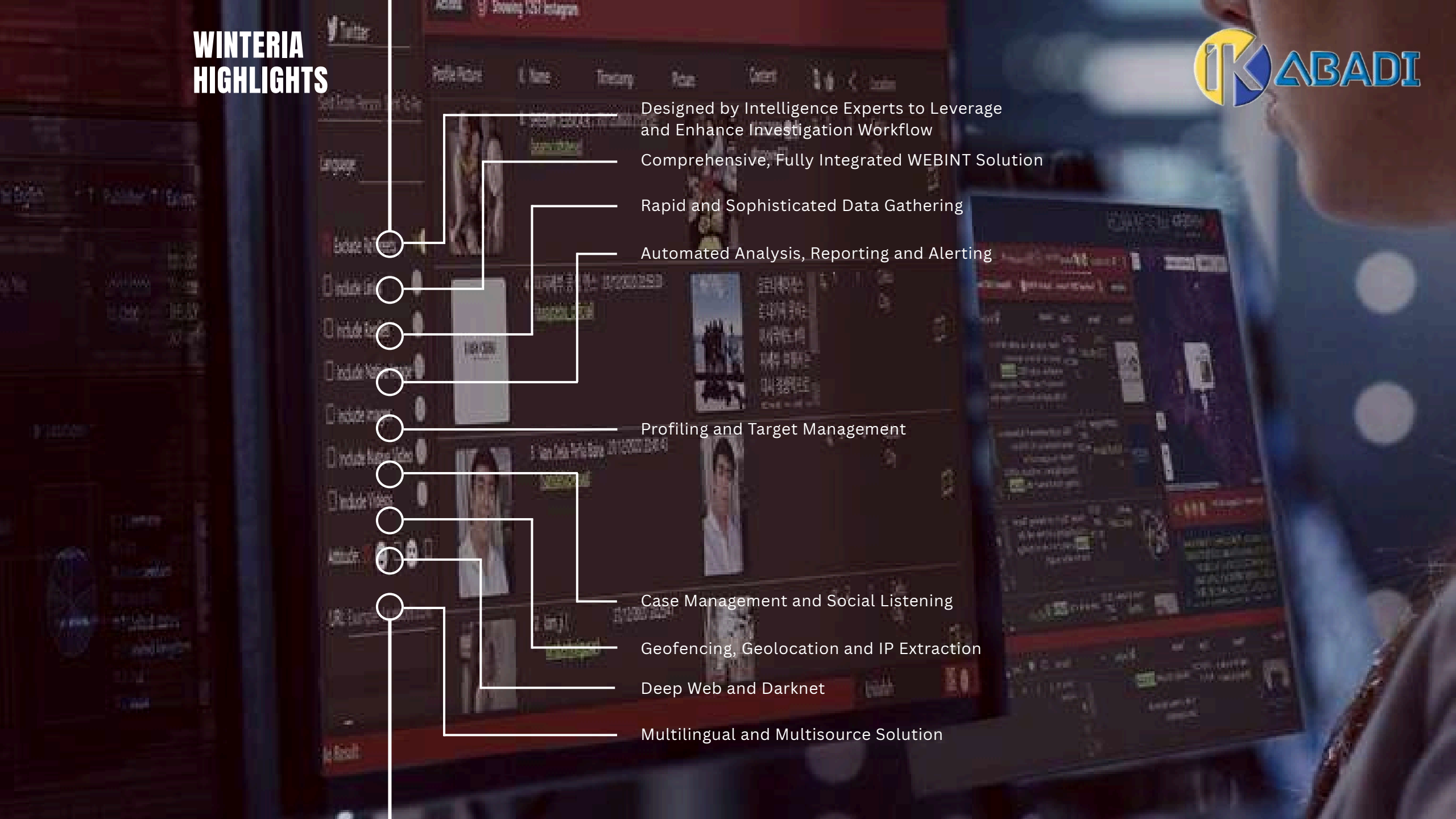
WINTERIA Compass is a unique social-based IP extraction tool, aimed at uncovering targets' IP address and their estimated geolocation via advanced technology and distinctive Virtual HUMINT methods, without interception or any offensive actions. The tool requires establishment of minimal Virtual HUMINT communication with the target via instant messaging applications, hence the IP address alongside the precise timestamp, and the estimated geolocation of the target can be automatically extracted.

DARKNET SEARCH

WINTERIA Dark dives into the deepest waters of the internet and uncovers the most protected and clandestine online discourse, to support broad intelligence operations from financial intelligence to Cyber Threat Intelligence. Throughout exclusive private sources and unique collection methods, WINTERIA Dark engages in the darknet, extracts, and analyzes the discourse according to the given credentials and the intelligence requirements. Keep your finger on the pulse of the darkest matters of the internet.

WINTERIA HIGHLIGHTS

- Designed by Intelligence Experts to Leverage and Enhance Investigation Workflow
- Comprehensive, Fully Integrated WEBINT Solution
- Rapid and Sophisticated Data Gathering
- Automated Analysis, Reporting and Alerting
- Profiling and Target Management
- Case Management and Social Listening
- Geofencing, Geolocation and IP Extraction
- Deep Web and Darknet
- Multilingual and Multisource Solution



INTELEGENT INTEGRATED SYSTEM

BUSINESS EMAIL PROTECTION

Secure corporate email in the cloud and on-premises from even the most sophisticated attacks

Block all email- borne attacks with one intelligent solution

Email is often the initial point of compromise in major security incidents. Threat actors effectively have unlimited attempts to succeed and only need to trick one unsuspecting user to gain a foothold in the corporate network.

Business Email Protection detects and blocks all email attacks, including sophisticated attacks that legacy solutions and third-party email providers often miss. Business Email Protection defends against every email-borne t hreat, from spam and phishing to malware delivery and business email compromise.

KEY FEATURES & BENEFITS

Attachment & Link Analysis

Inspect over 290 different file formats to ensure all attachments are safe. Check all links, including obfuscated and redirected links.

PAYLOAD DETONATION

Detonate and analyze suspicious attachments and links in isolated environments, stopping attacks at their roots

ANTI-EVASION TECHNIQUES

Utilize advanced detonation technologies to stay one step ahead of cybercriminals in their attempts to evade detection.

ATTACKER ATTRIBUTION

Cross-check detonation reports with Group-IB's Threat Intelligence to attribute attacks to specific threat actors or malware families

ANTI SPAM & ANTI PHISHING

Block spam and phishing attacks to prevent credential theft, malware infection on end-user workstations, and other potential risks

FLEXIBLE DEPLOYMENT

Get to full deployment quickly with a flexible solution that can be SaaS, self- hosted in the cloud, or hosted in a fully isolated on-prem installation

DIGITAL RISK PROTECTION

Attachment & Link Analysis

The Digital Risk Protection platform leverages advanced technologies to detect the illegitimate use of logos, trademarks, content, and design layouts across the digital surface.

Automatic identification

The Digital Risk Protection platform leverages advanced technologies to detect the illegitimate use of logos, trademarks, content, and design layouts across the digital surface.

Machine learning that detects violations at earliest stages

- Identifies fraud and scam before the traffic attraction stage
- Continuously enriches detection algorithms across industries
- Utilizes Graph module to map and takedown entire fraud networks

HOW DIGITAL RISK PROTECTION WORKS

Step 1

RESOURCE MONITORING

- Domain names
- Databases of phishing resources
- Search engines• Social media
- Mobile app stores
- Online classifieds and marketplaces
- Advertising• Instant messengers
- Deep/dark web
- Public databases and code repositories
- Breached databases

Step 2

VIOLATION D ETERMINATION

- Phishing• Scam
- Trademark violation
- Counterfeit
- Piracy
- Partner policy compliance
- Data leakage
- VIP impersonations

Step 3

RESPONSE

- Comprehensive takedown procedure reaching an 85% pre- trial takedown rate on average

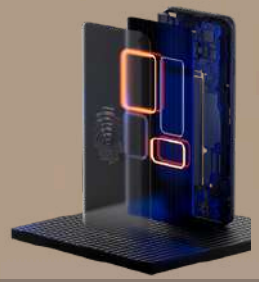
FRAUD PROTECTION

Eliminate fraud across all digital
channels in real time

- Credit card fraud
- Social engineering attacks
- Malicious bot activity
- E-commerce fraud
- Attacks on gaming/betting sector
- Malware-related fraud
- Money laundering
- Payment fraud

Web Channel Protection

- Anonymized user mouse/trackpad/ keyboard behavioral analysis
- Malware, bot and RAT detection
- Device technical specifications
- Device graphic and display configuration
- Browser configuration



Mobile Channel Protection

- Android or iOS operating system configuration monitoring
- Device sensor monitoring
- Mobile operator characteristics monitoring
- Malware, bot and RAT detection
- Anonymized user behaviour monitoring
- Device technical specifications

No crime unpunished

Entrust your case to Group-IB's Investigation Team

- Proprietary technologies for crime detection

- Global collaboration with law enforcement agencies

- Deep knowledge of criminal schemes

- Individual approach and special project teams

More than detection

Integration with Threat Intelligence receives the following data:

- IP Intelligence data: TOR, proxy, hosting

- Phishing and malicious domains
- Malicious software behaviors and signatures

- Compromised user accounts

- Compromised payment cards

No bad bots allowed

Preventive Proxy protects web and mobile applications from various types of bot activity, including:

- Mobile API attacks

- Unauthorized use of API

- Automation framework detection

- Scraping

- Brute force

- Credential stuffing

- Layer 7 DDoS

- Cookie theft

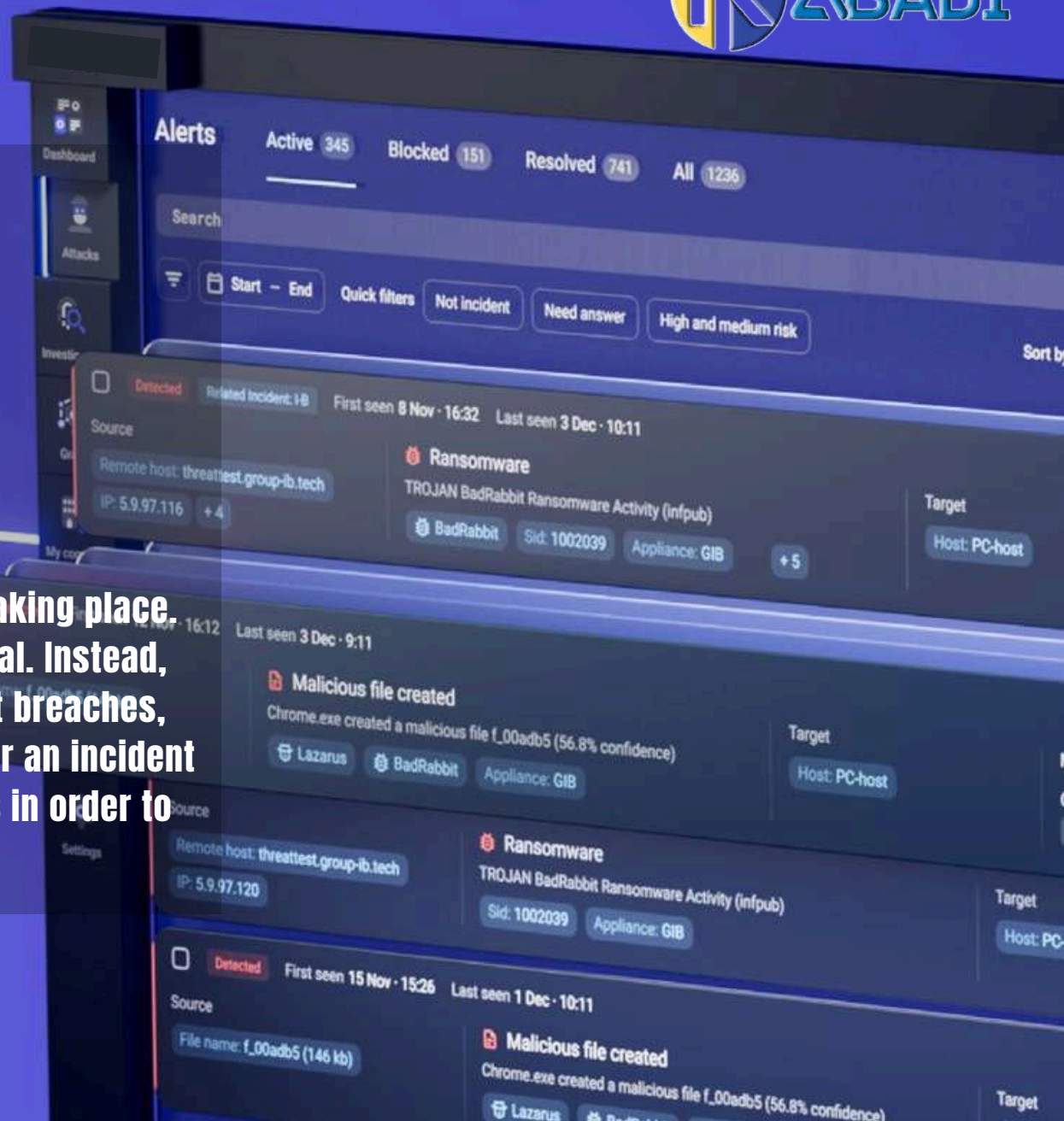
MANAGED XDR

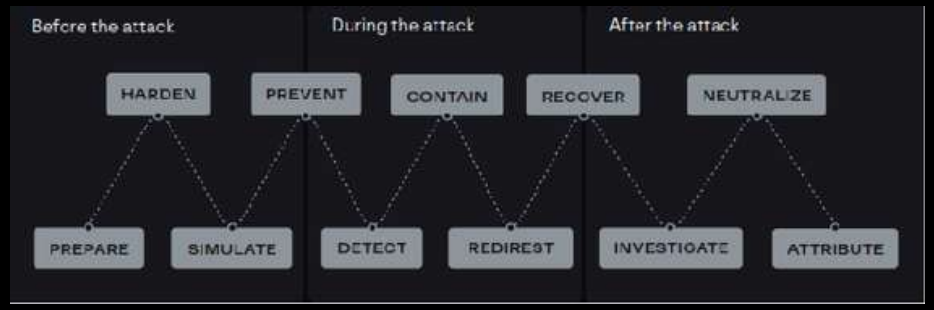
Supercharge security and defeat attacks before they begin with knowledge of how and when you will be attacked

A new set of security objectives

Cyber response chain

Security teams are no longer expected to prevent breaches from taking place. In today's threat landscape, prevention simply is not a realistic goal. Instead, security teams today are assessed by how quickly they can detect breaches, limit the blast radius, and minimize the mean time to recovery after an incident occurs. Security teams must manage the following chain of events in order to apply these new metrics:





Time is of the essence

Breaches are unavoidable, so a fast response is imperative. The longer it takes to discover and respond to an incident, the more expensive it is to fully recover from it.

Managed Extended Detection and Response (XDR)
A faster and more efficient product class

XDR solutions were designed to leverage both the increasing number of telemetry sources and the everevolving ML algorithms, providing superior detection and response capabilities.

Empowered with malware detonation, threat intelligence, and ML models for event correlation, Group-IB Managed XDR works seamlessly across networks, endpoints, and clouds in order to make the effectiveness of your security operations greater than the sum of their parts.

Managed XDR overcomes the most pressing security challenges in today's world

Eases alert fatigue

Thousands of security events take placeevery hour. Group-IB XDR correlates data and identifies the issues that require action.

Extends limited resources

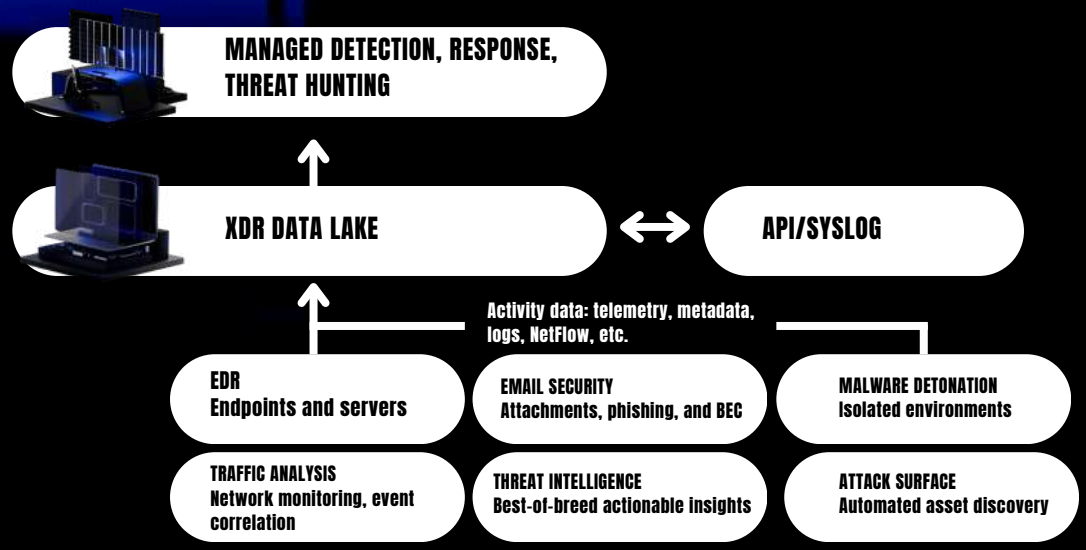
Security teams are often overtasked andunder-resourced. Use Group-IB XDR to ease workflows by streamlining detection and response.

Connects siloed solutions

Managing a portfolio of security solutions is difficult and time-consuming. Every component of Group-IB XDR works in unison to increase ROI.

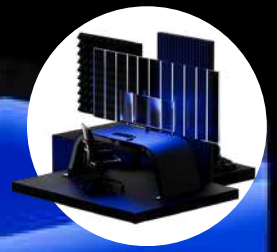
Keeps up with evolving threats

Cyberattacks are constantly evolving and becoming more sophisticated. To keep up with them, leverage intelligence insights and advanced tech.



Extend your security team

Strengthen your security posture with Managed Detection, Managed Incident Response, and Managed Threat Hunting capabilities



Managed detection

Offload internal teams with 24/7 CERT. Our team will analyze alerts and provide you with actionable recommendations on relevant threats

Managed incident response

Mitigate threats and get a faster response with DFIR experts leveraging XDR capabilities to collect forensic data and implement remote response actions

Managed threat hunting

Detect yet undiscovered threats and APTs and let expert threat hunters test hypotheses based on XDR data to give you full visibility over your security postur

Managed XDR Features

Endpoint Detection and Response Endpoints	• Host-level detection • Behavioral ML-classifiers • Streamlined response • Application control	• Asset inventory • UEFI threat detection • Forensic data collection
Network Traffic Analysis Network	• L2-L7 protocol support • Network logging and metadata collection • Custom rules • Detection of covert channels (DNS-, ICMP-tunneling, DGA)	• Encrypted traffic analysis (ETA) • C2 traffic and server discovery • Extraction of objects for analysis
Malware Detonation Files and links	• Automatic VM customization • Object analysis across infrastructure • 290+ supported object formats • Link analysis	• Retrospective analysis • Anti-evasion technologies • Actionable in-depth reports
Malware Detonation Email Protection Malware, spam, and BEC attacks	• On-prem or fully cloud deployment • Anti-spam filtering • AV analysis • Realistic VMs (image morphing)	• Network tunneling • Advanced anti-evasion • Post-delivery protection • BEC and phishing detection
Managed Services Detection, response, and threat hunting	• 24/7 alert monitoring • False positives triage • Direct connection with analysts • Personalized threat landscape	• Hypothesis testing • Custom playbooks for IR • Experts at hand

THREAT INTELLIGENCE

Supercharge security and defeat attacks before they begin with knowledge of how and when you will be attacked

Threat Intelligence provides unparalleled insight into your adversaries. Integrate the intelligence to maximize the performance of every component of your security ecosystem. Equipping your team with Group-IB's strategic, operational, and tactical intelligence streamlines security workflows and increases efficiency.

Strategic intelligence

- Revolutionize risk management with bespoke on-demand, and regular monthly and quarterly threat reports written by analysts specifically for the board and executive business cases
- Enable growth with actionable threat intelligence before expanding into a new region / business line, and get industry-specific threats before digital transformation
- Lower the cost of cyber security by avoiding unnecessary purchases and postponing upgrades by maximizing the efficacy of your existing security investment

Operational intelligence

- Transform security and adapt instantly, use the insights to block malicious network and endpoint activity the moment it is first observed anywhere in the world
- Identify and remove weaknesses before they are exploited by conducting Red Teaming with detailed knowledge of threat actor's tools, tactics and processes
- Automate workflows and improve team efficiency by enriching your SIEM, SOAR, EDR and vulnerability management platforms with outof-the-box integrations for Group-IB threat intelligence

Tactical intelligence

• Prioritize vulnerability patching for your technology stack with automated alerts that inform you the moment vulnerabilities are discovered or begin being exploited by threat actors targeting your industry
• Eliminate false positives and focus on legitimately risky events with a continuously updated database of system and network indicators of compromise for cybercriminals in your threat landscape
• Reduce response time with complete information about the cyber kill chain in the MITRE ATT&CK® matrix format, use the information to quickly remove them from your network

KEY FEATURES

Graph interface

Investigate and research threats with an intuitive graphical interface. Use the Graph to easily explore the relationship between threat actors, their infrastructure and the tools they use at a glance and drill into the details with just a click.

Compromised data detection

Discover compromised credentials, including VIP's personal accounts, payment card information and breach databases before they are used to launch attacks or cause financial damage. Alerts within can be created to inform you whenever a compromise for your organization is discovered.

Dark web insights

Group-IB's Unified Risk Platform has the industry's largest dark web database, access into intelligence with Threat Intelligence to discover illegal activities and monitor whether your organization is mentioned on the dark web. Create rules to inform you when a topic of interest is discussed.

Phishing detection and response

Configure the Unified Risk Platform with Group-IB Threat Intelligence to automatically detect and takedown malicious websites automatically to protect your brand and customers. Mitigate damage caused by phishing in record time thanks

Threat actor attribution

Easily understand threat actors' behaviors, preferred methods and infrastructure with insight into their activity in the MITRE ATT&CK format. The Unified Risk Platform tracks and logs their attacks in real-time; review these insights within Group-IB Threat Intelligence.

Malware and vulnerability investigation

Use Group-IB Threat Intelligence to detonate suspicious files on the Unified Risk Platform or submit them to our reverse engineering team. Review in-depth analysis of the weaknesses targeted by malware and threat actors from the dashboard to prioritize patching.

Tailored threat landscape

Track threat actors easily with a customized threat landscape dashboard, giving you a single pane of glass to monitor their attacks. Use the landscape to track actors that target you, your industry, partners, clients and those of interest.

Comprehensive integrations

Enhance your existing security ecosystem easily with out-of-the-box integrations for the Unified Risk Platform with popular SIEM, SOAR, and TIP solutions, or via API and STIX/TAXII data transfer to any tool in your security ecosystem.

Comprehensive intelligence powered by the Unified Risk Platform

Open-source intelligence
- Paste sites
- Code repositories
- Exploit repositories
- Social media discussions
- URL sharing services

Malware intelligence
- Detonation platform
- Malware emulators
- Malware configuration files extraction
- Public sandboxes

Sensor intelligence
- ISP-level sensors
- Honeypot network
- IP scanners
- Web crawlers

THREAT INTELLIGENCE

UNIFIED RISK PLATFORM

Human intelligence
- Malware reverse engineers
- Undercover dark web agents
- DFIR and audit services
- Law enforcement operations
- Regional specialists

Vulnerability intelligence
- CVE list
- Exploit repositories
- Dark web discussions
- Threat campaigns mapping

Data intelligence
- C&C server analysis
- Darkweb markets
- Darkweb forums
- Instant messengers data (Telegram, Discord)
- Phishing and malware kits
- Compromised data-checkers

AI-Driven WEBINT

Tap into the world's largest database - the Internet
Unlock valuable insights

What is DEEP WEBINT?

Introducing GoldenSpear AI-Driven WEBINT, the pinnacle of advanced intelligence tools available in today's market. We have skillfully blended the power of artificial intelligence and cutting-edge WEBINT technology to create a system that takes data gathering, analysis, and presentation to a whole new level.

Primarily designed to support law enforcement, intelligence agencies, businesses, and researchers, our AI-powered OSINT system ensures precision and speed, diving into vast pools of publicly accessible data, uncovering relevant information as it emerges in real-time.

GoldenSpear's AI-Driven WEBINT is the fruit of decades of R&D, adeptly architected to process massive volumes of data instantaneously. With it, our users gain the power to access critical information just when they need it most, all with an unrivaled level of accuracy.

AI-Driven WEBINT

Tap into the world's largest database - the Internet
Unlock valuable insights

Unique Features

Flexible and Configurable

GoldenSpear's AI-Driven WEBINT is engineered with versatility at its core. Adapt the tool to your unique requirements with our flexible and configurable features, ensuring it works exactly how you need it to.

Privacy-Oriented Design

We prioritize your privacy. Our tool is designed with built-in privacy support, safeguarding your activities while you focus on the critical task at hand.

Secure Browsing Enhanced by RBI

Experience enhanced online security with our remote browser isolation (RBI) feature. This feature o ers an extra layer of protection, ensuring secure browsing by isolating your browsing activities from your local systems and networks. With GoldenSpear's AI-Driven WEBINT, surf the web confidently, knowing that your cyber safety is our priority.

Comprehensive Website Downloads

Our tool supports full website downloads, enabling comprehensive evidence capture. Never miss a piece of vital information as you gather digital evidence.

User-Friendly Graphical Interface

Leveraging intuitive design principles, we have developed a user-friendly graphical user interface (GUI). This ensures a seamless interaction between you and the tool, making complex data collection and analysis tasks straightforward and e cient. Our intuitive GUI is designed to reduce the learning curve and enhance productivity, empowering users of all technical levels to master our tool with ease. With GoldenSpear's AI-Driven WEBINT, experience the perfect blend of power and simplicity

- Background Information and Vetting
- Investigation and Evidence Collection
- Lead Generation
- Threat Intelligence
- Counter Intelligence
- Monitoring Online Activity

Key Benefits for

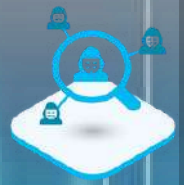
Key Benefits for Intelligence Teams

Identifying Suspects

DEEP WEBINT allows law enforcement to quickly and easily search for suspects by analyzing publicly available data sources such as social media profiles, online forums, and news articles

Monitoring Criminal Activity

DEEP WEBINT can be used to monitor criminal activity online, track the movements of suspects, and analyze communication between suspects



Monitoring Criminal Activity

Darknet Monitoring Uncover data breaches, online fraud, cybercriminal tactics and other threats to your organization by accessing many darknet forums and marketplaces. movements of suspects, and analyze communication between suspects

Improving Public Safety

DEEP WEBINT can help law enforcement monitor social media and other online sources for threats to public safety, allowing them to respond quickly to potential threats.

Enhancing Intelligence Gathering

DEEP WEBINT tool can be used to gather intelligence about potential threats, such as terrorist organizations or cyber criminals, by analyzing online activity and communication.

Social Listening

Monitor and Analyze trends and online conversations about topics, brands, and products across various social media platforms.

Gathering Evidence

Law enforcement can use DEEP WEBINT to gather evidence that can be used in court, such as social media posts, online photos, and videos.

Investigating Financial Crimes

DEEP WEBINT can help organizations investigate financial crimes such as money laundering or fraud by identifying suspicious financial transactions or undeclared assets.

Tracking Missing Persons

Law enforcement can use DEEP WEBINT to search for information about missing persons, such as their last known location, and analyze social media and other online activity for clues.

Collaboration and Sharing

DEEP WEBINT can be used to collaborate and share information between different law enforcement agencies, allowing for more efective and eticient investigations.

DeepContra.

ABADI

Combining Deepfake Detection with Open Source Intelligencefor Digital Integrity

Our integrated platorm, combining Deepfake Detection with Open Source Intelligence (OSINT) capabilities, stands at the forefront of this battle against digital deception. By harnessing the most advanced artificial intelligence and machine learning algorithms, our Deepfake Detection solution is meticulously designed to identify, analyze, and neutralize deepfake content and other forms of manipulated media. This cuting-edge technology empowers organizations across various sectors to preserve their integrity and trustworthiness in the digital landscape, ensuring that the truth prevails in an era where reality and fabrication often intersect.

Simultaneously, our OSINT Platform elevates the capability to conduct comprehensive investigations into the origins and spread of digital content, making informed decision-making and proactive risk management achievable. With a robust suite of tools that

Collect, analyze, and leverage publicly available data from a myriad of online sources, our platform providesactionable insights and a contextual understanding that is unparalleled. It enables organizations to navigate the complexities and nuances of the digital world with enhanced confidence and clarity. Together, these integrated solutions offer a holistic approach to confronting and overcoming the challenges posed by digital misinformation, ensuring a more secure and trustworthy online environment for all.

Capability Overviews

Detection of Manipulated Multimedia Content

The platform employs advanced AI-driven algorithms and multimedia analysis techniques to scrutinize audio, video, and image content across major social media platforms like Twitter, Facebook, Instagram, Tiktok, and Youtube.

Analysis of Deepfake Creators

The system is capable of not just idetifying deepfake content but also tracing the origins of such content back to its creators by analyzing the content and omparing detected faces with official records.

Evaluation of Social Media Account Authenticity

The system offers a robust mechanism for evaluating the authenticity of users on various social media platorms, discerning real identties from fake ones and identifying bot-operated accounts.

Impact Measurement of Fake or Bot Accounts

The system offers a sophisticated framework for measuring the impact of fake or bot accounts on social media, particularly concerning their influence on public opinion.

Identification of Altered Images

The platform is equipped with so phisticated AI and graphics processing tools designed to detect alterations in images posted on social media platforms, even if the changes are subtle and made with advanced tools like Photoshop.

Source Determination of Deepfake Material

The platform leverages advanced scraping and data collection techniques to determine the source and omponents of deepfake content found on social media.

Sentiment Change Alerts and Keyword Tracking

The platform is capable of sending alerts when there's a significant shift in public sentiment towards specific topics or hashtags. It also tracks keyword mentions on social media and detects emerging movements orchestrated by fake accounts.

Data Analysis on Viral Content

The platform is adept at providing comprehensive data on viral content or hashtags, identifying their origins and the initial accounts responsible for sharing them.

Conversation and Activity Analysis

The system is proficient in analyzing the volume and nature of conversations and activities across various social media platforms, offering insights into sentiment trends and how they correlate with trending topics.

In-depth Account Behavior Research

The platform conducts comprehensive research on account behavior, assessing the level of risk, public geolocation, and recent activity to provide a detailed profile for security analysis.

Social Media Reach Measurement

The system measures the reach of each social media account and highlights those that are particularly influential within a conversation, pinpointing key players in the social media landscape.

Recognition of Viral Images in Conversations

The platform employs object and face recognition technologies to identify and track viral images in conversations, including frequently appearing mocks, faces & logos.

User Engagement Analysis

The system analyzes user engagement based on connections, behaviors, and subjects to identify profiles with high interaction & community influence.

Detection & Filtering of Spam Content

The system is equipped to detect & filter out spam content, including posts containing malicious phishing URLs, ensuring the safety and integrity of content on social media platforms.

Demographic Data Presentation

The platform presents comprehensive demographic data about all social media users involved in a conversation, offering valuable insights into the audience's composition.

Theme and Influence Analysis

The system analyzes the main themes and identifies influential subjects discussed by social media users, uncovering the core topics and key influencers shaping social media narratives.

Geolocation Data Display & Filtering

The platform displays publicly available geolocation data for social media conversations and allows for targeted filtering by region, offering localized insights.

GoldenSpear
DEEP FUSION
Supporting AML & Crypto Investigation

Functionality

- Access to blockchain information
- Ingestion of user provided
- Financial transaction information (through multisource data integration)
- Search capability
- Link analysis
- Display on map
- Real time monitoring and alerts
- Automatic compliance reporting
- Ability to combine WEBINT investigation with financial investigation.

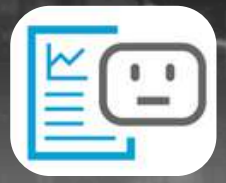
DEEP FUSION

Deep Fusion is a cutting-edge data analytics platform that leverages S2T's expertise in Web Intelligence (WEBINT) and combines it with sophisticated machine learning algorithms, dynamic data integration, and advanced visualization tools. This novel platform is designed to empower law enforcement, financial institutions, and regulatory bodies in the battle against financial crimes such as money laundering, especially within the cryptocurrency domain. Deep Fusion is our answer to the escalating complexity of financial crime. It represents an innovative approach to data analysis, a fusion of artificial intelligence and human insights that aims to provide an unparalleled view into the vast and complex web of financial transactions.

Key Benefits

Unparalleled Data Integration

Deep Fusion seamlessly integrates disparate data sources, both structured and unstructured, from local databases to the vast and complex world of the web, including social media, news articles, blogs, and even the dark web. This allows for an all-encompassing view of potential criminal activity.



Advanced Analytics and AI-driven Insights

Using advanced machine learning algorithms, Deep Fusion identifies patterns, anomalies, and connections that would be virtually impossible for humans to detect manually. Our platform provides predictive and prescriptive analytics, helping users not just to understand the past and present, but also to anticipate future threats.

Real-time Monitoring and Alert System

Deep Fusion o ers a robust real-time monitoring and alert system that tracks suspicious activities & high-risk entities, providing immediate notifications to users for swift action.

User-friendly Visualization Tools

With Deep Fusion, complex data is transformed into clear, intuitive visualizations, maps, and graphs. This allows for easier analysis and interpretation of data, even for non-technical users.

Compliance and Reporting

Deep Fusion streamlines the compliance process, with features that automate report generation in line with the latest AML regulations, ensuring your organization remains compliant at all times.

Deep Fusion's robust capabilities make it an ideal tool for various applications, including:

Fraud Detection

Deep Fusion can be used to identify patterns that indicate fraudulent activity, helping organizations to mitigate risks and prevent financial loss.

Anti-Money Laundering (AML)

Deep Fusion helps identify, monitor, and report suspicious transactions, facilitating the detection and prevention of money laundering activities.

Regulatory Compliance

Our platform not only helps in detecting and preventing financial crime but also ensures that your organization stays compliant with changing AML regulations.

Cryptocurrency Investigation

With the rise of cryptocurrencies, understanding their transaction flow is critical. Deep Fusion tracks & analyses these transactions, helping to reveal hidden patterns, detect fraudulent activities & identify suspicious entities.

Threat Intelligence

Deep Fusion's advanced analytics can be used to gather threat intelligence, providing a deeper understanding of potential threats and enabling proactive security measures.

How Does it Works

The system has direct access to blockchain, with the following platforms:

- Bitcoin
- Ethereum
- Bitcoin Cash
- Dash
- Litecoin
- Zcash
- Ziliga
- BNB Smart Chain
- Tron
- Stellar
- Dogecoin
- XRP
- Ethereum Classic

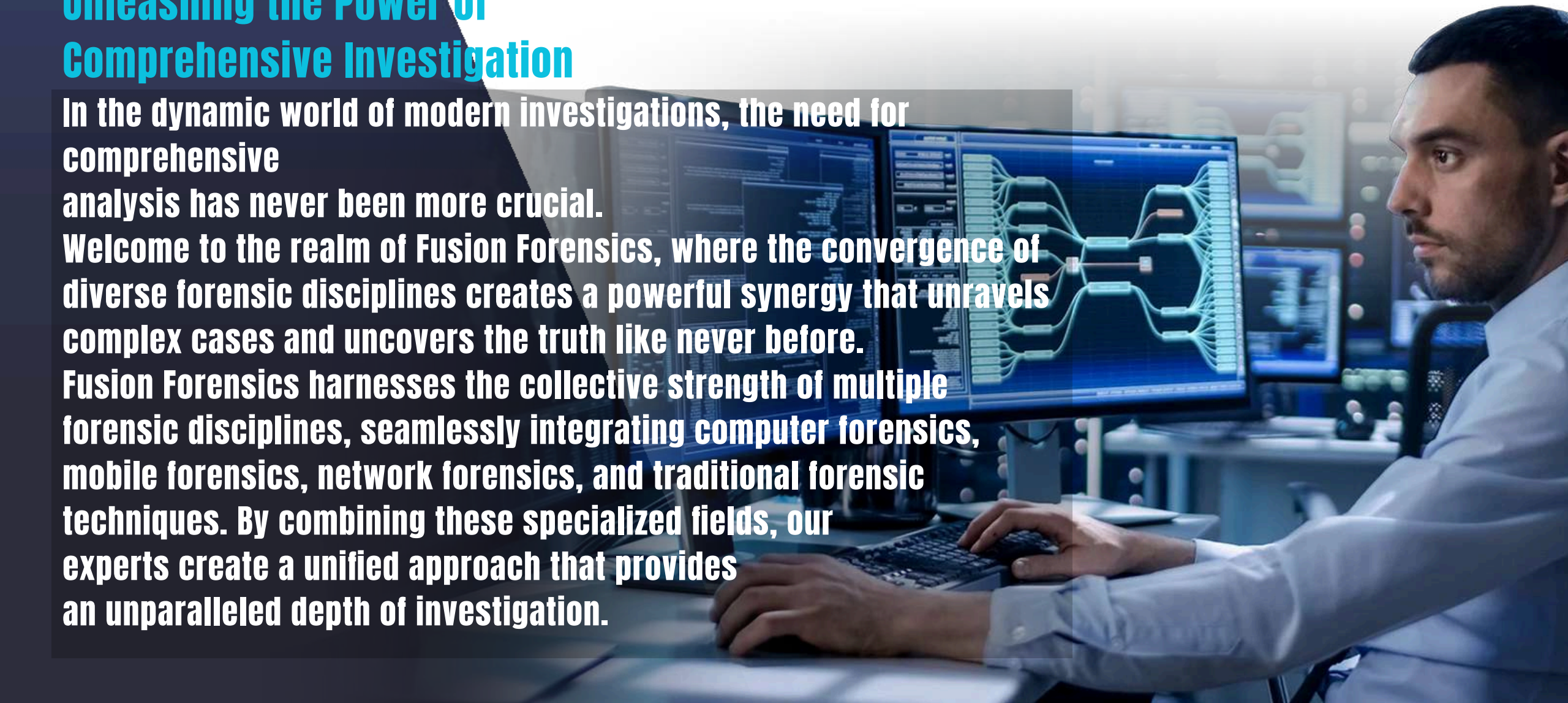
The system can also identify names of currencies and blockchain wallet addresses within WEBINT or other content.

The system is also able to ingest financial transactions, e.g. Suspicious Transaction Reports (STR) in XML format and allow users to conduct AML investigations or other financial investigations.

Fusion Forensics

Unleashing the Power of Comprehensive Investigation

In the dynamic world of modern investigations, the need for comprehensive
analysis has never been more crucial.
Welcome to the realm of Fusion Forensics, where the convergence of diverse forensic disciplines creates a powerful synergy that unravels complex cases and uncovers the truth like never before.
Fusion Forensics harnesses the collective strength of multiple forensic disciplines, seamlessly integrating computer forensics, mobile forensics, network forensics, and traditional forensic techniques. By combining these specialized fields, our experts create a unified approach that provides an unparalleled depth of investigation.



Features

- Incident response and digital evidence preservation
- Forensic data acquisition and analysis
- Network intrusion and cyber-attack investigation
- Mobile device forensics, including smartphones and tablets

Goldenspear Foresight

Empowering Strategic Intelligence with Advanced Predictive

In today's rapidly evolving geopolitical landscape, timely and accurate intelligence is crucial. Goldenspear Foresight is an advanced geostrategic intelligence platform that combines cutting-edge technology with expert analysis to provide a comprehensive understanding of global events. By leveraging Bayesian networks for predictive analytics and conducting thorough horizon scanning, we help organizations anticipaterisks and make informed decisions

Advantages

Proprietary Algorithms
Highlight that your platform uses proprietary algorithms developed in-house for higher accuracy in predictive analytics and risk assessment.

Hybrid AI Models
Mention that "Goldenspear Foresight" combines multiple AI techniques, such as Bayesian networks, machine learning, and natural language processing, to provide a more nuanced understanding of geopolitical events.

AI-Driven Scenario Planning
Include a feature that uses AI to generate multiple future scenarios based on current data, helping users prepare for a range of possible outcomes.

Unique Applications and Use Cases

Disaster Response and Humanitarian Aid
Introduce capabilities specifically designed for disaster response and humanitarian aid organizations, such as predicting natural disasters or tracking refugee movements.

Economic and Market Impact Analysis
O er specialized tools for analyzing the economic and market impacts of geopolitical events, helping businesses better understand the implications for their operations.

Collaborative Decision-Making Tools
Introduce features that facilitate collaboration among team members, such as shared workspaces, discussion boards, and collaborative scenario planning.

Key Features

Real-Time Event Monitoring

Stay ahead of global developments with our real-time event monitoring system. Goldenspear Foresight tracks and visualizes events as they unfold, providing instant insights into geopolitical shifts, diplomatic actions, and emerging conflicts. This feature allows decision-makers to react swiftly and accurately to changing circumstances.

Advanced Predictive Analytics with Bayesian Networks

Harness the power of Bayesian networks to model complex relationships and predict future geopolitical events. Our advanced predictive analytics engine identifies patterns in data, evaluates probabilities, and forecasts potential outcomes, enabling proactive risk assessment and strategic planning.

Comprehensive Horizon Scanning

Utilize horizon scanning to detect early warning signals of potential threats and opportunities. Goldenspear Foresight continuously scans a wide range of data sources—such as economic indicators, social media trends, and news feeds—to identify emerging trends and geopolitical risks. This proactive approach ensures you stay one step ahead in an unpredictable world.

Dynamic Event and Relation Maps

Visualize global relationships and interactions with our interactive event and relation maps. Understand the connections between countries, organizations, and key actors, and analyze the implications of their actions. This feature provides a clear picture of the geopolitical landscape, highlighting areas of potential conflict or cooperation.

Dynamic Event and Relation Maps

Visualize global relationships and interactions with our interactive event and relation maps. Understand the connections between countries, organizations, and key actors, and analyze the implications of their actions. This feature provides a clear picture of the geopolitical landscape, highlighting areas of potential conflict or cooperation.

In-Depth Actor Analysis

Gain insights into the behavior and motivations of global actors with our in-depth actor analysis tools. Goldenspear Foresight assesses the roles, intentions, and influences of key players, helping you anticipate their actions and understand the broader context of international relations.

Risk Assessment Tools

Improve your risk management strategies with our sophisticated risk assessment tools. By analyzing a variety of factors—including political stability, economic conditions, and military capabilities—our platform helps you evaluate potential risks and prepare for future scenarios.

Applications

Government and Defense

Utilize Goldenspear Foresight for national security, strategic planning, and threat assessment. Our platform's real-time monitoring and predictive capabilities ensure you are always prepared to respond to global challenges.

Corporate Risk Management

Mitigate geopolitical risks that could impact your business operations. Goldenspear Foresight's horizon scanning and risk assessment tools provide the intelligence needed to safeguard your interests and maintain business continuity.

Research and Academia

Enhance your research capabilities with access to comprehensive geopolitical data and advanced analytical tools. Goldenspear Foresight supports thorough analysis and provides valuable insights into global trends and events.

SINGULARITY ENDPOINT

Autonomus, Next-Gen EPP and EDR

As digital landscapes transform, the speed, sophistication, and scale of threats against endpoints have also evolved. User endpoints remain a key attack vector for malicious actors seeking deeper access to your network. Simultaneously, security analysts are overwhelmed with the sheer number of false positives and alerts, which requires time-consuming manual investigation. Security teams need a more efficient and robust solution to secure every endpoint in their environment.

Singularity Endpoint combines next-gen prevention with real-time detection and response in a single platform with a single agent, empowering security teams to easily identify and secure every user endpoint on their network.

Industry-Leading Endpoint Protection

Deliver unparalleled endpoint protection and detection with broad visibility, rapid response times, and minimal incident dwell time. As evidenced in the 2022 MITRE Engenuity™ ATT&CK® Evaluation, SentinelOne delivered 100% protection and detection with zerodelays and the highest analytic coverage in real-time.

Quickly Contain Attacks With Built-in Automation

Patented Storyline™ technology provides analysts with real-time actionable correlation and context. Analysts can understand the full story of what happened in the environment with automatic linking of all related events and activities together with a unique identifier. Automate response to affected endpoints to reduce the mean time to respond. Autonomously resolve threats with our patented one-click remediation to reverse all unauthorized changes.

Streamlined Security

Investigate, triage, and hunt with zero learning curve to bring IR and hunting to a broader pool of security talent. Uplevel SOC resources for proactive threat hunting with automated hunting rules, intel-driven hunting packs, and support for MITRE ATT&CK techniques. Easy-to- use search and pivot lighten analyst load to hunt across large volumes (up to 3+ years) of EDR telemetry.

Key Benefits

Protect

Protect endpoints in real-time

Detect

Detect threats without human intervention

Respond

Remediate threats with 1-click or automated or response actions

+ AI-based malware and ransomware protection
+ Patented 1-click remediation and rollback
+ Industry-leading coverage for Windows, Mac, and Linux, including legacy OSes
+ Mobile endpoint support for iOS, Android, and ChromeOS
+ Autonomous operation. Works on- and off-network
+ Hunt by MITRE ATT&CK" Technique
+ Flexible EDR data retention up to 3+ years
+ Rapid deployment interoper-ability features ensure a fast, smooth rollout.
+ Single cloud-delivered platform with true multi-tenant capabilities to address the needs of global enterprises and MSSPs

PURPLE

Your AI security analyst to detect earlier, respond faster, and stay ahead of attacks

Today’s security teams are dealing with a sophisticated threat landscape and endless alert queues that grow far faster than what teams can even hope to resolve. It’s labor-intensive, precludes any proactive threat hunting, and leads to burnout and missed alerts.

Purple AI is the industry’s most advanced AI security analyst that translates natural language into structured queries, summarizes event logs and indicators, guides analysts of all levels through complex investigations with recommended next questions and auto-generated summary emails, and scales collaboration with shared investigation notebooks—ensuring rapid detection, investigation, and response.

Unlike other solutions that act as a console chat bot, Purple AI is a force multiplier that helps analysts conduct faster, better investigations with:

+ One-click threat hunting quick starts based on the latest threat intelligence
+ Intelligent suggested next queries to continue your hunt
+ Lightning fast queries and visibility of native and third party data in a single view
+ Shared investigation notebooks to collaborate across teams
+ Direct answers to Sentinel One support questions so you don't have to search online documentation

Unlock Your Security Team's Full Potential

Simplify the Complex

Streamline investigations by intelligently combining common tools, synthesizing threat intelligence and contextual insights into a single conversational user experience.

Uplevel Every Analyst

Find hidden risk, conduct deeper investigations, and respond faster—all in natural language. Train analysts with power query translations from natural language prompts.

Take Hunts from Hours to Minutes

Accelerate SecOps with our patent-pending hunting quick starts, AI-powered analyses, auto-summaries, and suggested queries. Save time by seamlessly collaborating on investigations in saved and shareable notebooks.

Safeguard Your Data

Leverage a solution designed for data protection and privacy by design. Purple AI is never trained with customer data and is architected with the highest level of safeguards.

The Purple AI Difference

+80%

Faster threat hunting & investigations
as reported by early adopters

Speed & Visibility with One Console, Platform, & Data Lake

Accelerate operations and see the full picture more clearly with one console, one platform, and the industry's most performant data lake. Purple AI is the only AI analyst that understands OCSF logs—so you can instantly query native and partner data in a single normalized view.

Threat Hunting Quickstarts & Guided Investigations

Help every analyst reduce MTTD and proactively find risk with our patent-pending hunting quick starts library. Leverage intelligent, contextually-suggested next queries to continue investigations in natural language.

Accelerate Collaboration Across the Board

Auto-generate threat summaries, reports, and communications that can be shared across teams and cut down on unnecessary back
and forth by collaborating in saved, shared, and editable notebooks.

Open & Reliable AI

AI shouldn’t be a black box.
With Purple AI, you can easily view query translations for verification and analyst training. Purple AI is also carefully architected with guardrails that protect against misuse and hallucinations.

Key Features

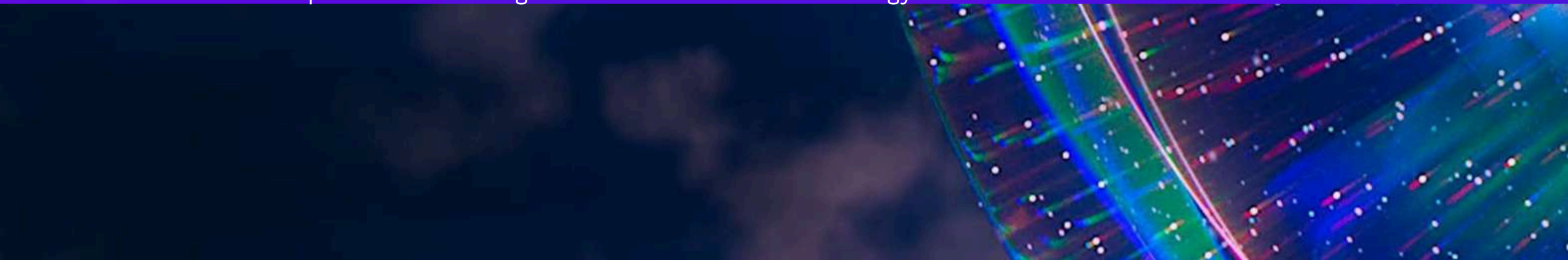
- Translate natural language into structured PowerQueries to search for hidden risk. Get outcomes you can trust with full views of queries and summarized results in natural language.
- Patent-Pending Threat Hunting Quickstarts enable analysts to proactively hunt for threats with a single click, using pre-populated queries based on our leading threat intelligence.
- Lightning fast queries and greater visibility. Built on top of the Singularity Data Lake, Purple AI is the only GenAI analyst that supports the Open CyberSecurity Schema Framework (OCSF) to provide native and third party data in a single normalized view.
- Conduct deeper investigations with suggested, contextual follow-on queries.
- Surface actionable insights faster with AI-powered threat analyses and summaries.
- Refer back to auto-saved private investigations notebooks or boost collaboration on hunts across teams in shared notebooks.

SINGULARITY XDR

Extend Protection, Detection, and Remediation to Endpoint and Beyond

The cybersecurity threat landscape is evolving exponentially in both speed and scope. Meanwhile, most security teams struggle to keep pace with emerging threats with the resources they have at hand. These organizations often lack global visibility and context across their technology stacks, creating gaps in what they can see and detect. Simultaneously, analysts juggle point tools for each vector, forcing them to analyze data in isolation and manually investigate. Today's security teams need a more proactive solution to identify, contain, and remediate emerging threats.

SentinelOne Singularity XDR unifies and extends detection and response capabilities across multiple security layers, including endpoint, cloud, identity, network, and mobile, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated response across a large cross-section of the technology stack.



Comprehensive Coverage Across Your Enterprise Stack With Operational Simplicity

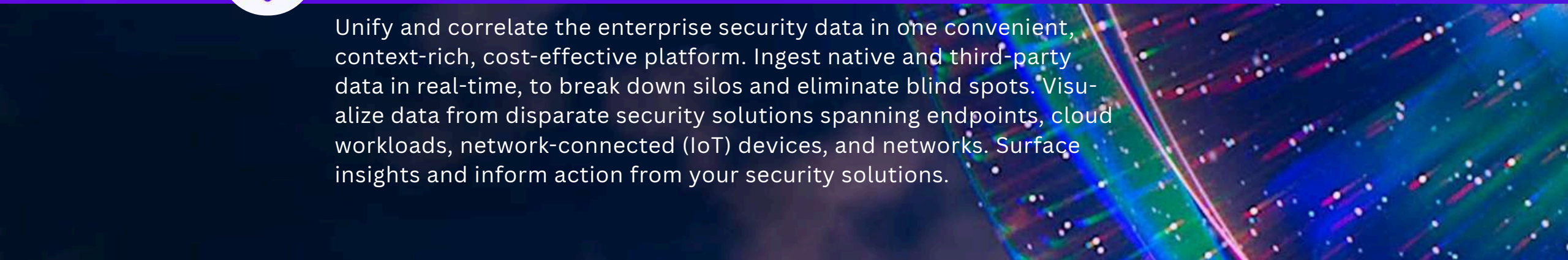
Deliver native protection across multiple solutions, including endpoint, cloud, identity, mobile, and devices. It enables frictionless third-party integrations, including threat intelligence, SIEM, SOAR, email, SASE, sandbox, and more, enabling you to leverage your existing investments.

Increased Security Team Efficiency

Auto-correlate individual events into an attack sequence, to streamline investigation and response. Analysts can automatically resolve threats with one click, without scripting across the estate. Execute orchestrated remediation actions in a single step, including network quarantine, auto-deploy agents on unprotected workstations, or automate policy enforcement across cloud environments.

Streamline Security Workflows Powered by a Unified Data Store

Unify and correlate the enterprise security data in one convenient, context-rich, cost-effective platform. Ingest native and third-party data in real-time, to break down silos and eliminate blind spots. Visualize data from disparate security solutions spanning endpoints, cloud workloads, network-connected (IoT) devices, and networks. Surface insights and inform action from your security solutions.



Key Benefits

See

Maximize visibility across every corner of the enterprise

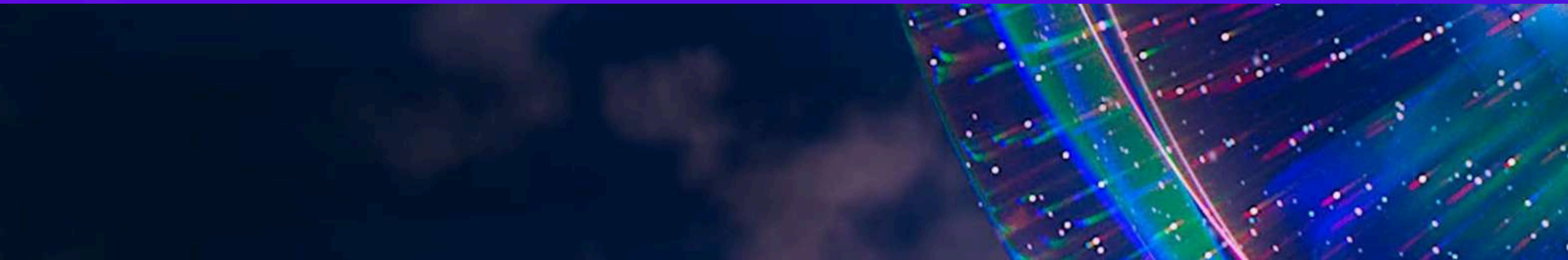
Protect

Protection coverage with unrivaled speed, efficiency, and simplicity

Resolve

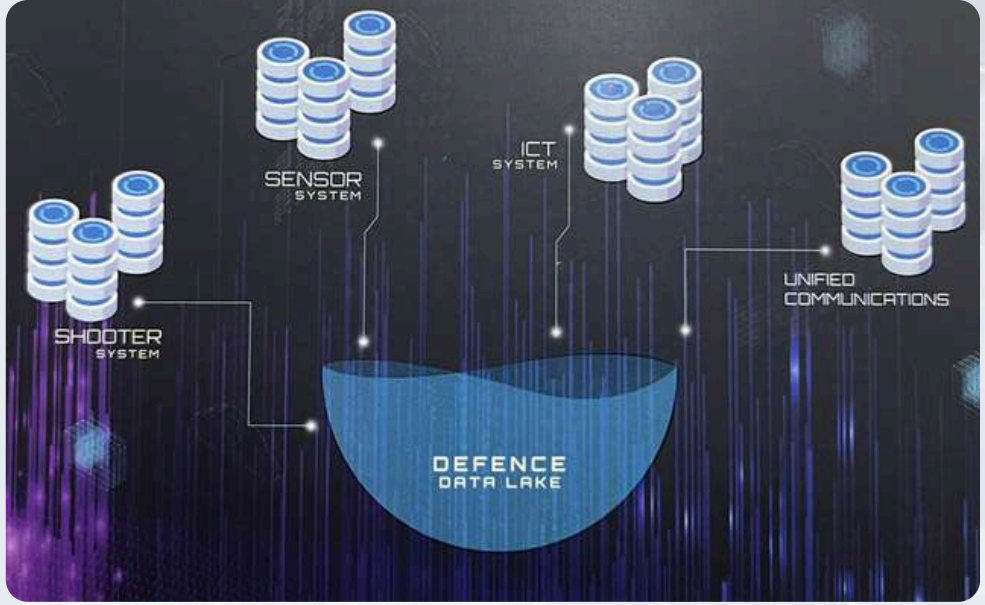
Automate response across the entire connected security ecosystem with a single click

+ Streamline operations andsecurity workflows
+ Reduce mean time to respond with simple, fast, and relevant automation
+ Up-level analyst productivity
+ Accelerate time to value for security analysts
+ Combine native and open XDR to offer customers the flexibility they need without limiting them to one solution multi-tenant capabilities to address the needs of global enterprises and MSSPs



C5ISR

(COMMAND AND CONTROL, COMMUNICATION, COMPUTER AND CYBER WARFARE INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE)



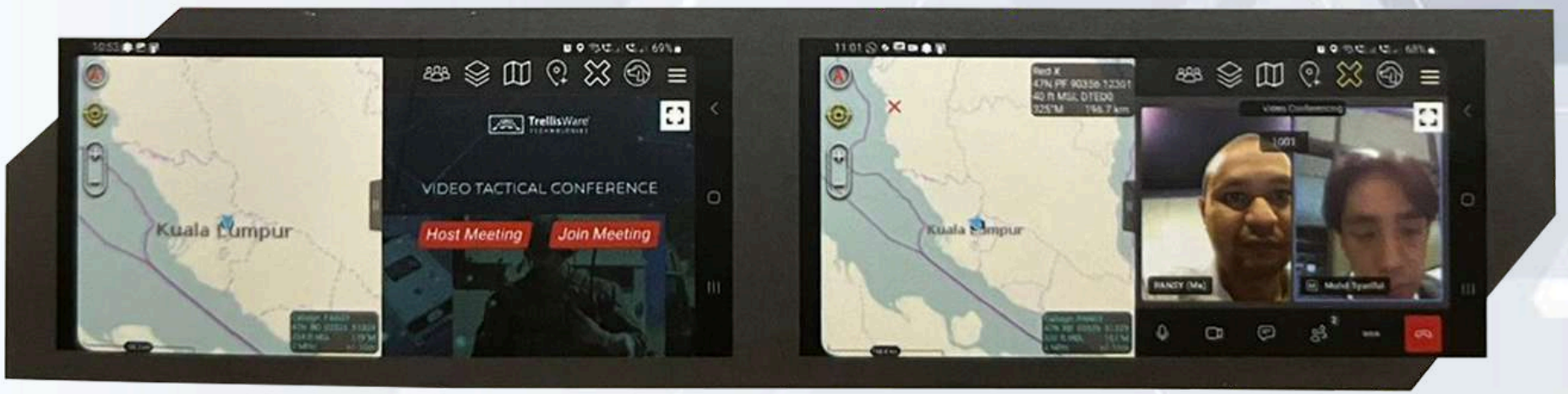
DEFENCE DATALAKE

A major benefit for all military branches in using data lakes is access to a secured data source that is rich in diversity but also well-aligned to the missions across the military, leveraging the standardization of data stream schemas that are used within the Defence organization to avoid the disorganized "data graveyard." Using data lakes will translate into massive time savings and the ability to leverage industry-grade machine learning and artificial intelligence applications for deployment. The Army, Navy, Air Force, and most sectors within the Defence organization could use data lakes to drive wart are intelligence in a significant way. Imagine how much more powerful our military will be with the ability to access mission relevant information, analyze it and push it out quickly, potentially opening exponential opportunities to predict enemy moves, assess inventory, plan and execute routine or abrupt maintenance. Decision-makers could predict when and where enemy forces will act against us, putting our commanders in an advantageous position to win battles and weaken enemy threats. Though the defense sectors have suffered from a challenging acquisition model in the past, the future looks bright because data lakes will provide a mission-critical advantage to our military services if we choose to embrace it.

SERVICES

Our company possesses extensive expertise and a proven track record in successfully executing complex system integration projects, particularly in the realm of military systems, radar technology, C2 (Command and Control) systems, and AAK (Android learn Awareness Kit) Integration Service. Our comprehensive capabilities encompass seamless integration, ensuring interoperability and enhanced functionality for mission-critical applications across these diverse systems

C2 (COMMAND AND CONTROL) SYSTEM



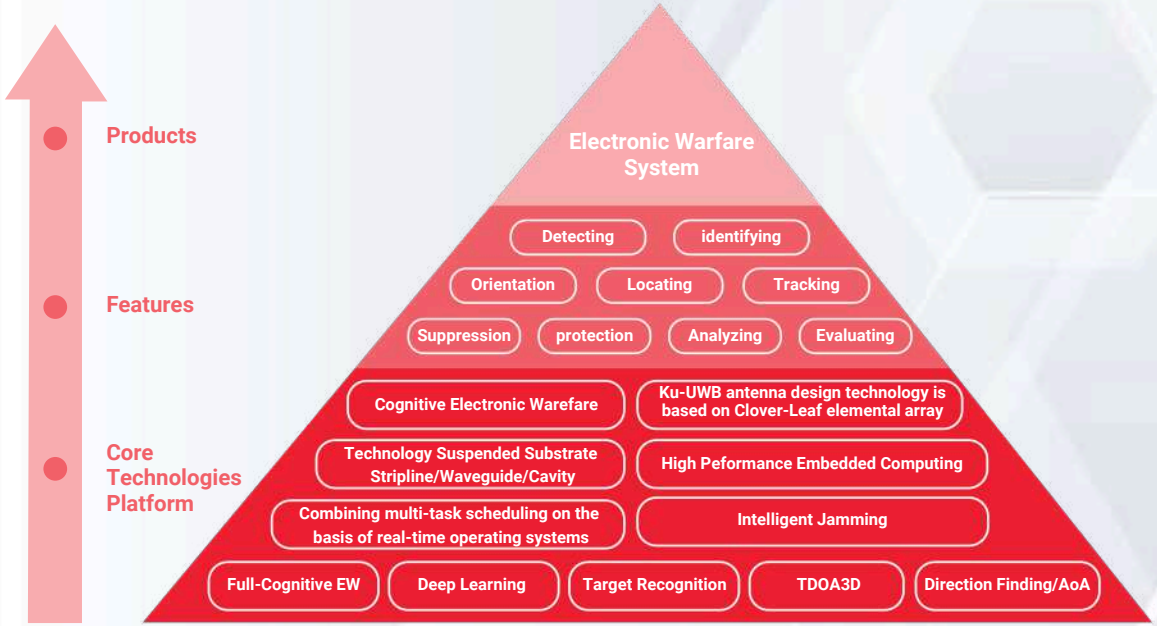
ATAK (ANDROID TEAM AWARNESS KIT) INTEGRATION SERVICE

- The system leverages the extensive capabilities of any secured network to ensure optimal user accessibility, making it easier to access operations from the appropriate team or source.

- The system is seamlessly implemented using a lightweight framework that aligns perfectly with the current technology capabilities and resources available to the users.

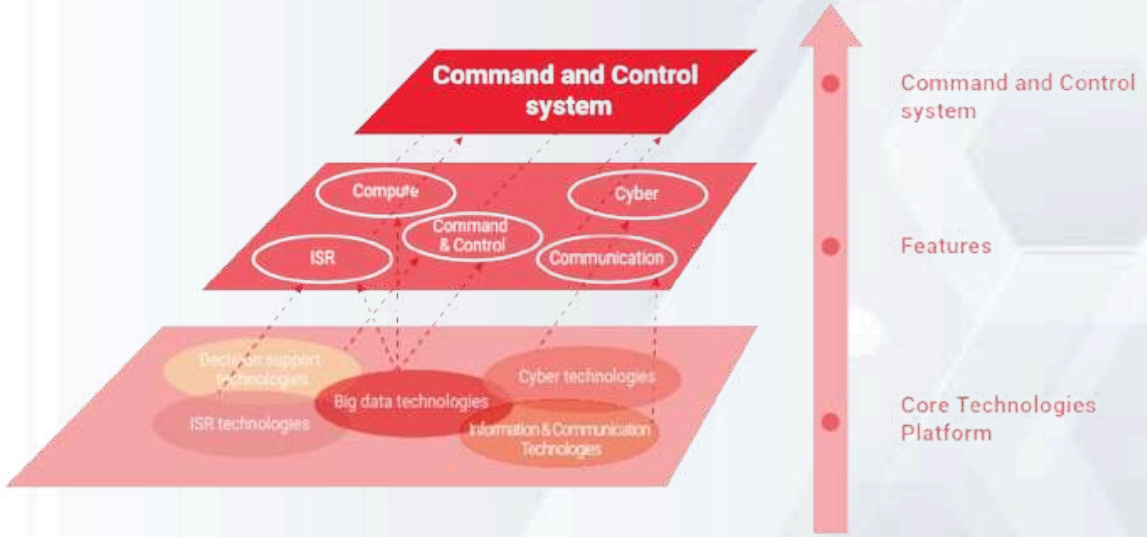
- The system leverage advanced analytics and machine learning models to extract valuable insights from the data. This includes predictive analysis, anomaly detection, sentiment analysis, and more. These insights can be used for mission planning, threat detection, resource allocation, and strategic decision-making.

ELECTRONIC WARFARE



In modern warfare, electronic warfare becomes an important factor in winning the war. Electronic warfare is a means of multiplying power and is one of the three major parts of high-tech warfare, including both offensive and defensive, and as such, countries have invested much in creating electronic warfare systems. These systems are capable of detecting, locating, tracking, classifying, and identifying communication signal sources and radar pulse emissions, designed to equip electronic warfare forces. developing the 3rd and 4th generation Intelligence electronic warfare product lines (Cognitive Electronic Warfare), including lines of electronic reconnaissance, electronic suppression and electronic protection, operating in a wide frequency range, ensuring modern and effective combat capabilities in the electronic field. warfare products are designed to ensure the following factors: **OPEN:** The products are designed with wide to super wide spectrum; including radio, infrared, optical, ultraviolet spectrums allowing dealing with all types of signals and targets. Software defined radio allows easy, fast addition and update of signal processing algorithms. **COMPACT:** The products are designed on a highly modular basis allowing easy optimization of designs for workstations, vehicle-mounted, drones or carry-on. The carry-on or hand-held product lines are optimally designed in terms of size, weight and energy consumption. **CONNECT:** Standardizing the design allows products to easily connect to each other to become an effective combat system as well as connect to headquarters at all levels according to the standard model of C5ISR. **INTELLIGENCE:** The products can collect, analyzing, decoding and processing big data (big data analysis); applying machine learning that allows automatic processing of test replacement when necessary.

COMMAND AND CONTROL SYSTEM



Researched and developed command automation systems to the 5th generation to perform command, control and computing tasks in the C5ISR combat model. These systems are responsible for displaying the entire picture of the combat situation, processing, analyzing and supporting the commander to make quick and accurate decisions. Corporation's Command and Control system is built on mastering the most advanced technologies available today, at the same time, building its own hardware model for the system by separating the components in the C5ISR system into discrete services and functions such as: Connecting Communication, Command & Control, Computing, ISR, Cyber along with the respective technology platforms. Also orients the development of Command and Control systems focusing on the following factors:

- Open architecture, broad system scalability, capable of integrating different combat units, transmitting information and delivering orders to each soldier, attaching equipment to the system to ensure real-time combat coordination.
- Building a communication platform for the system with the following features: Wireless transmission, Transmission in low bandwidth conditions, transmission with high reliability. With the foundation and achieved results, Program is forming a "multi-domain" command and control product: On the ground, at sea, in the air, in electromagnetic space, in cyberspace, connecting the entire command automation system of the arms of the whole army into an overall system.

AIR FORCE, AIR DEFENSE COMMAND AND CONTROL SYSTEM

GENERAL INTRODUCTION

Air Force, Air Defense Command and Control System is an automated system of command and control for air defense and air force operations. The system provides the commander with a picture of situation in the air, supporting the commander to make timely and accurate operational decisions.

KEY FEATURES

Situational Awareness
• Collect, process and gather information from military radars, civil radars and other intelligence sources.
• Provide Recognized Air Picture (RAP) and transmit to other related units.
Support Decision-making Process
Air Defense Tactical support
• Collect, process information, warn and assess the level of danger of flying targets.
• Calculate and display the combat capabilities of air defense units.
• Calculate and display system generated solution for weapon assignment, resources, equipment,...
• Exchange and Transmit information, commands and reports among levels.
Air Force Guidance.
• Maintain and manage continuity of operations
• Create manual tracks and support training. • Manage systems (users, combat units...).
• Support data-recording mode and re-display in two modes:

SPECIFICATIONS

Numberof concurrent targets Track update rate	Thousands
Number of concurrent Flight plan Management	< 5 seconds Thousands
Number of concurrent connected radar/ station	Hundreds
Number of concurrent guided aircrafts	Hundreds
Time for dividing and assigning target among fire units	< 20 seconds
Operating systems	Linux based

NAVY COMMAND AND CONTROL SYSTEM

GENERAL INTRODUCTION

Navy Command and Control System is an automated system that provides situational awareness to naval forces in order to enhance their decision-making and provide a tactical advantage in complex environments.

KEY FEATURES

Collect, process, and merge information from sources in the air, sea, and underwater in real time, build a comprehensive picture of the sea:

- Provide situational awareness.
- Friend or Foe units Tracking.
- Manage Battlefield Information.
- Tabular Display and Graphical Display on Digital Map.
- Support Mission Planning.
- Monitor Tasks operation.
- Monitor Operational and Logistics Status.
- Manage Reports and Messages.
- Decision Support.
- Sensor Management.
- Interoperability with Other Armed Forces Systems.

SPECIFICATIONS

Number of concurrent targets	Hundreds of thousands
Track update rate	< 30 seconds
Number of concurrent calculation targets	Thousands
Number of proposed actions per target	Dozens
Transmit and monitor command execution	Yes
Time of data-recording storage	Up to 12 months

NAVY COMMAND AND CONTROL SYSTEM

GENERAL INTRODUCTION

• Electronic warfare command and control system is an automated system of command and control for Electronic Warfare Operations.
• The system provides the commander with a picture of situations in air, navy and land, supporting the commander to make timely and accurate operational decisions.

KEY FEATURES

- Connect and collect information from reconnaissance electronic warfare units.
- Process information and build a recognized electronic picture.
- Automatically analyze, assess and report reconnaissance electronics in real time.
- Evaluate the threat and warning unusual activities.
- Transmit command from commander to Subordinate units.
- Support data-recording and re-display data in the Electronic Situation Display.
- Support to build operational and training plans.
- Interoperability with Other Armed Forces Systems.

SPECIFICATIONS

Number of concurrent targets	Thousands
Target's information update rate	< 5 seconds
Digital Map Time of data	Yes
recording storage Operating	Up to 90 days
System	Linux based

THE AUTOMATED SYSTEM FOR COLLECTING, ANALYZING AND LINKING EVENTS AND ENTITIES FROM THE INTERNET

KEY FEATURES

Our system collects, extracts, and analyzes data from digital news and social media to provide comprehensive and interconnected news updates between prominent entities and events. Key features include:

- Entity recognition
- Event detection, classification, and extraction
- Duplicate detection and tracing article's origin
- Automated timeline generation
- Identification of hot and prominent events
- Automatic data collection related to keywords
- Display of information in tabular format or graphics on digital maps
- Alerting based on event's interest level
- Statistics, reports, and news bulletins.

GENERAL INTRODUCTION

- The automated system for collecting, analyzing, and linking events and entities from the internet is a system that automatically collects and extracts information from various sources such as news and social media.
- Using the most powerful natural language processing technologies, our system automatically classifies content, extracts and identifies entities/events that are currently happening or about to happen, to serve various purposes: early detection and warning, monitoring, and tracking when information starts appearing on news and social media.

SPECIFICATIONS

Number of news sources collected simultaneously	Unlimited
Type of news sources	Online newspapers, forums, blogs, social media
Information collection frequency	< 5 minutes
Entity identification accuracy	Up to 90%
Entity of monitored keywords at the same time	Up to 20 keywords
Deployment method	On-premise/ User account/ Data service

CYBER WARFARE PLATFORM

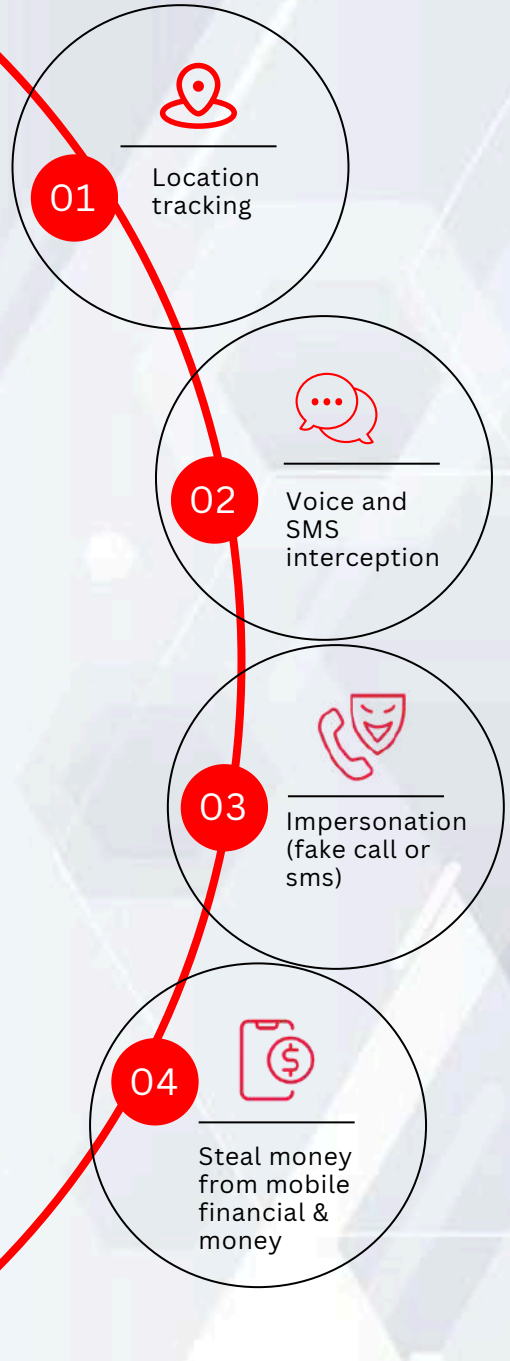
GENERAL INTRODUCTION

The Cyber Warfare Platform excels at gathering information from various internet sources, including news portals, forums, personal blogs, and social media platforms like Facebook and YouTube. It then analyzes and synthesizes this data based on specific topics or targets, enabling organizations to quickly access and interpret data for timely decision-making.

KEY FEATURES

- By using advanced AI technologies like NLP, speech, and image recognition, our platform efficiently handles diverse multimedia data. Viettel's Cyber Warfare Platform boasts the largest data collection capability in Vietnam, encompassing virtually all major social media platforms with significant user bases.
- Furthermore, it incorporates state-of-the-art AI techniques for advanced data analysis and processing, ensuring accurate and timely news monitoring. A standout feature is its YouTube surveillance capability, which, combined with our years of research in audio-to- text conversion and facial recognition, enables in-depth and effortless monitoring, even down to the visual and audio content of videos.
- Key Functionalities:- Surveillance- Cyber information warfare - Network warfare
- Developed and deployed by: Intelligence Service Center
- Deployment: The platform has now been successfully deploy in several Defense units, enabling efficient information monitoring and management. The platform gathers information from news portals, forums, personal blogs, and social media platforms like Facebook and YouTube, analyzing and synthesizing data to enable timely decision-making.
- The Cyber Warfare Platform empowers organizations to stay ahead by delivering real-time insights from vast amounts of online data. With its ability to analyze and synthesize information from millions of social media accounts and news sources, our platform enables organizations to make informed decisions and safeguard their interests.

RISK
Subscribers



ANOMALY DETECTOR

RISKS

MOBILE NETWORK OPERATORS (MNO) SUFFER FROM:

- Revenue loss due to fraudulence
- Service down time
- Trouble with legal issues
- Customer Care cost rises

- Loss of reputation and trust from customers > lose subscribers
- Revenue loss due to configuration mistakes or system errors Business
- model and network situation are revealed to rival MNOs

BORDER ROAMING GATEWAY

Border Roaming Gateway
Full & flexible control for operation engineers

01 Able to create many types of border zone

02 Configurable border zone

03 Configurable roaming reject reason for foreign networks & mobiles

04 Configurable Border roaming control timer for each border zone

BENEFITS

Ensure national sovereignty

Reduce risk of losing money for subscribers and foreign currency payment for home country government

Prevent unwanted roaming cases to neighbor countries’ networks.

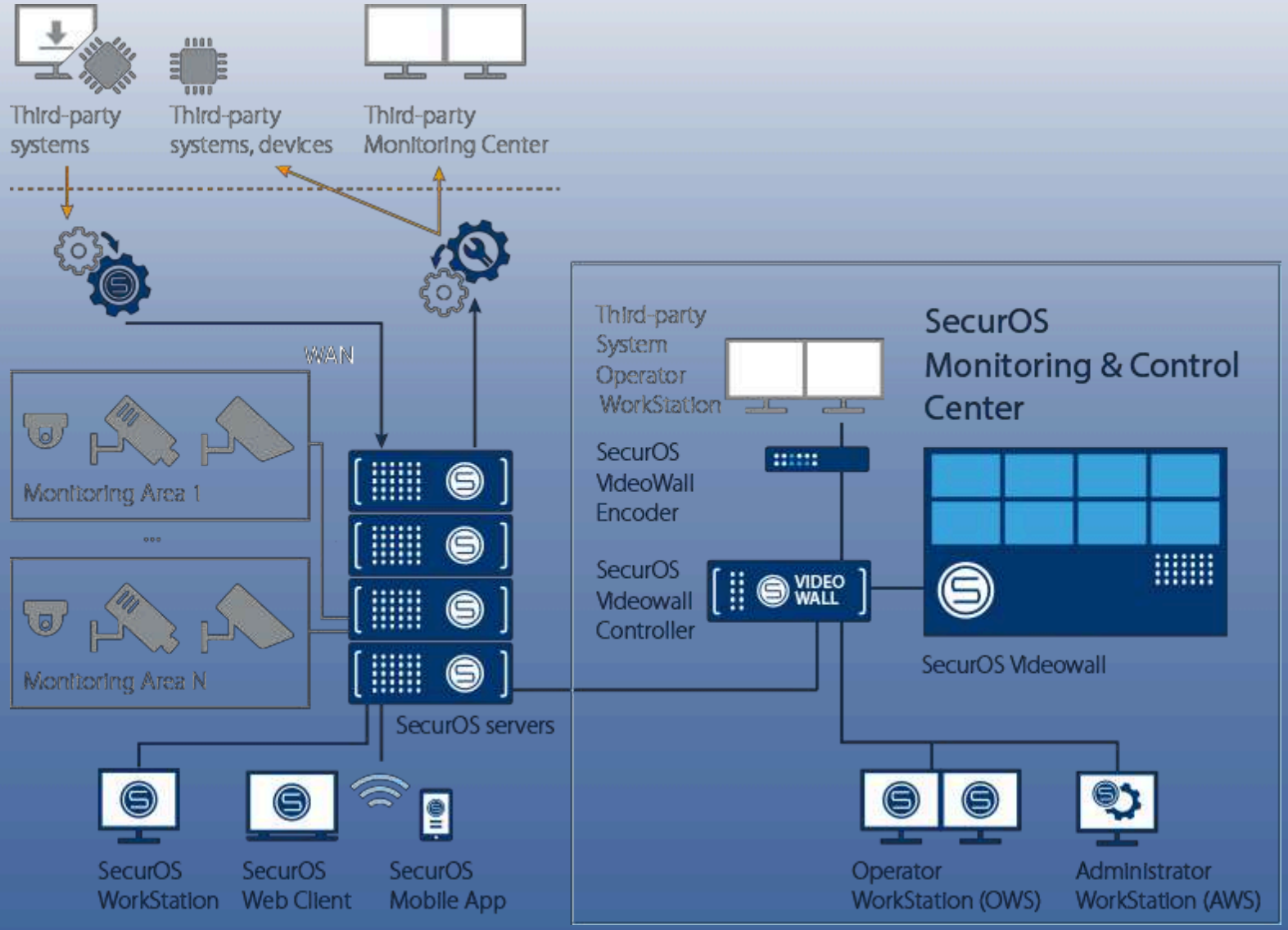
FACE AND BODY REGISTRATION, VIDEO ANALYTICS, INTELLIGENT SECURITY SYSTEM BASED ON AI AND CCTV

SECUROS
UNIDIED SECURITY & EXTENSIBULITY

By operating of both video management system and intelligent
analytics modules and detectors, SecurOS™ is the most powerful
framework in the world.

ISS advanced software and hardware based products and solutions portfolio

SECUROS - UNIDIED SECURITY & EXTENSIBULITY



SecurOS integrates a multitude of IS and third party systems into one integrated network and creates a unified command and control capability.

SECUROS - A COMPLETE SECURITY ECO-SYSTEM

FEDERATION
Support of local or distributed security systems into a unified network with unlimited numbers of video servers, cameras, sensors, etc. Centralized monitoring and control of local sites.

INTEROPERABILITY
Integrate third party systems and devices into
one network

ADDITIVE / MODULAR ARCHITECTURE
Scalable system topology generates ready ROI
on the system - new functionalities and capabilities can generally be added with minimal software management

EVENT / SCENARIO MANAGEMENT
Program complex reactions to complex events
to intelligently and dynamically react to real world events

EXTENSIBILITY / CUSTOMIZATION
From multi-layer maps, custom user-based screens and permissions, to custom forms and
GUI, SecurOS allows for complete customization based on user need

BUSINESS INTELLIGENCE
Advanced native analytics and integration of surveillance platform with business process systems allows for proactive action

SECUROS - TECHNOLOGICAL DOMINANCE

All devices, objects, cameras, systems, and even users, macros, and scripts can be individually managed and have multilevel permissions based on login.

Each object can be controlled manually or automated using scripts and macros

Security system efficiency active monitoring

Security system resources optimization

Continuity and redundancy capability with failover

Operating under insufficient capacity of data channels

Resilient data storage

High level of cyber-security

Full compliance with standards and requirements

INTERGRATIONS & COMPATIBILITY

- Video Cameras, incl. PTZ, fish-eye, ImmerVision, Computer Vision
- ACS, Security & Fire Alarms, Perimeter / Intrusion, Building Automation, Weight Stations, etc.
- Actuated equipment (sensors, beams, barriers, etc.)
- Video Walls
- Remote Storage / Data Centers (Virtualizations and NAS)
- GIS, Interactive 2D/3D Maps
- Emergency Service (911)
- PSIM, other 3rd-party software

NATIVE PRODUCTS

- License Plate Recognition
- Traffic Violations Detection Systems
- Face Capture & Recognition
- Train Character Recognition
- Sea Container Character Recognition
- Visual Inspection and Automation of Terminal Gates System
- Under Vehicle Surveillance System
- POS & ATM Transaction Monitoring
- Situational Awareness Video Analytics and Service Analytics
- Access Control & Fire Alarm
- Command & Control, Video Walls

MONITORING, FORENSICS AND MANAGEMENT

- Remote Monitoring and Admin
- Mobile App and WEB-browser
- Monitoring & Control Center
- Data Processing and Event Management
- SOL DB / XML
- ONVIF, RTP/RTSP, video formats: H.263, H.264, H.265, MPEG-4, MUPEG, MXPEG
- RestAPI / SDK/ IIDK / Active Media Kit (Video API)

LICENSE PLATE RECOGNITION

SecurOS Auto

Designed to effectively deal with different tasks related to control of parked/moving vehicles in law enforcement, commercial, and municipal organizations

- Template-based algorithms providing up to 98% recognition accuracy
- Video-based recognition, no loops required
- Regular updates for new plate types (templates)
- 15+ years of expertise. Proven to work in complex real life environment (day/night and wide range of weather conditions)
- Advanced Search capabilities: full or partial plate number including wildcard, search against watchlists and external databases
- Has full-featured user interface, which combines video from the LPR cameras with real-time PR events, search, watchlist capabilities, and more
- Designed for fixed and mobile installations
- Provides a number of unprecedented advantages for users, including the ability to accurately capture license plate information at 130 mph (210 km/h)

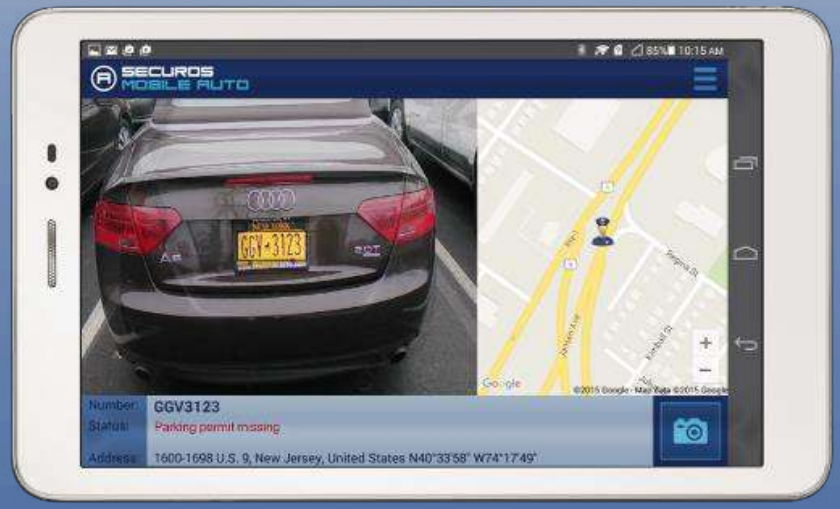
LICENSE PLATE RECOGNITION - RELATED SOFTWARE PRODUCTS

SecurOS EdgeAuto

A special integrated solution for LP/ANPR embedded on supported IP-cameras.
It is targeted for applications where the camera has a limited connection with the server, and it is necessary to perform real-time license plate recognition as well as have the corresponding video archive on the server for long-term storage.

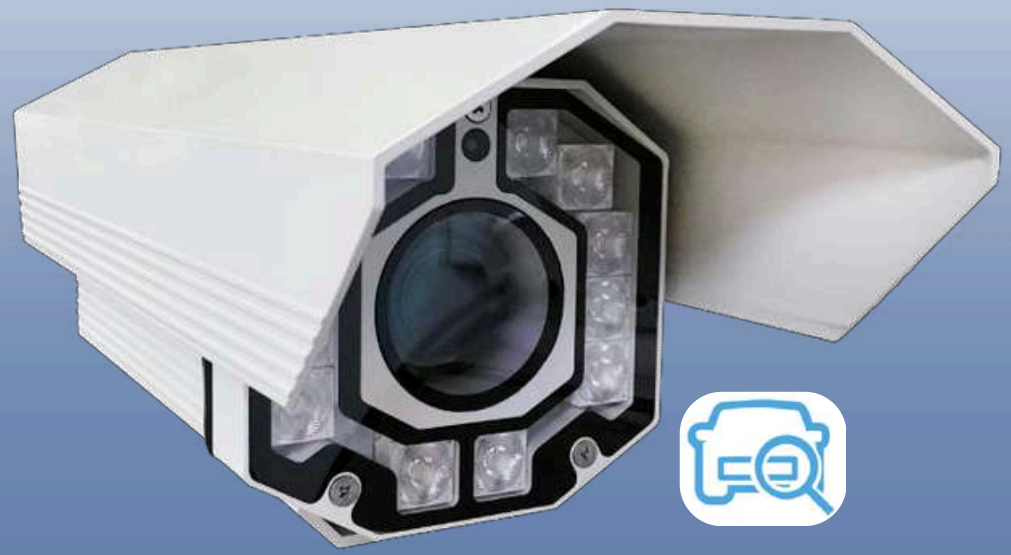
SecurOS MobileAuto

PR/ANPR mobile application designed for working in field conditions. The solution is intended for municipal and police authorities and the security services of commercial enterprises.



LICENSE PLATE RECOGNITION - SPECIALIZED TURNKEY SOLUTION

SecurOS Motus



SecurOS Motus 452 is an IP-based automatic license plate recognition camera designed for SecurOS Auto
- High-speed.
It provides unbeatable ANPR precision for commercial facilities and law enforcement applications.

- Ready-to-use all-in-one unit
- Specially designed for severe weather conditions
- Easy remote calibration and camera's configuration adjustments
- Built-in remotely configurable white-light or IR illuminator
- Superior image quality and NPR precision
- Recognize plates from two lanes of traffic
- IP67
- Adjustable wall-mount bracket is included
- Low power consumption
- FCC and CE certified
- 2 years warranty

ADVANCED SPEED LIMIT VIOLATIONS DETECTION

SecurOS Velox

SecurOS Velox is a ready-to-use all-in-one device designed for real-time traffic violations detection and automatic license plate recognition (ANPR) of all passing
vehicles - 24 hours a day under any weather conditions. SecurOS Velox provides automatic detection of traffic violations:

DETECTION OF COMPLEX TRAFFIC VIOLATIONS

SecurOS Crossroad

SecurOS Crossroad is an edge-to-edge solution for traffic violations detection. It combines specialized ruggedized hardware components and software for high precision detection and automatic license plate recognition (ANPR).

SecurOS Crossroad automatically detects a wide range of Traffic Violations at a crossroads including a violation failure to give way to pedestrians at zebra crosswalks.

SEA CONTAINER CHARACTERS RECOGNITION

SecurOS Cargo

SecurOS Cargo provides the ability to recognize characters on cargo containers from above, below, and from the side. It has an automated ISO code recognition system, so that the country of origin can be known right away. The advanced algorithms mean that such information can be read in any kind of weather, and can also read container characters on trucks as well as cranes.

By developing a container character recognition solution that integrates with cargo management processes at port, intermodal, and logistics centers, SecurOS Cargo can dramatically improve throughput and turnaround time, reduce liability, and be utilized to better locate and track containers in large facilities.

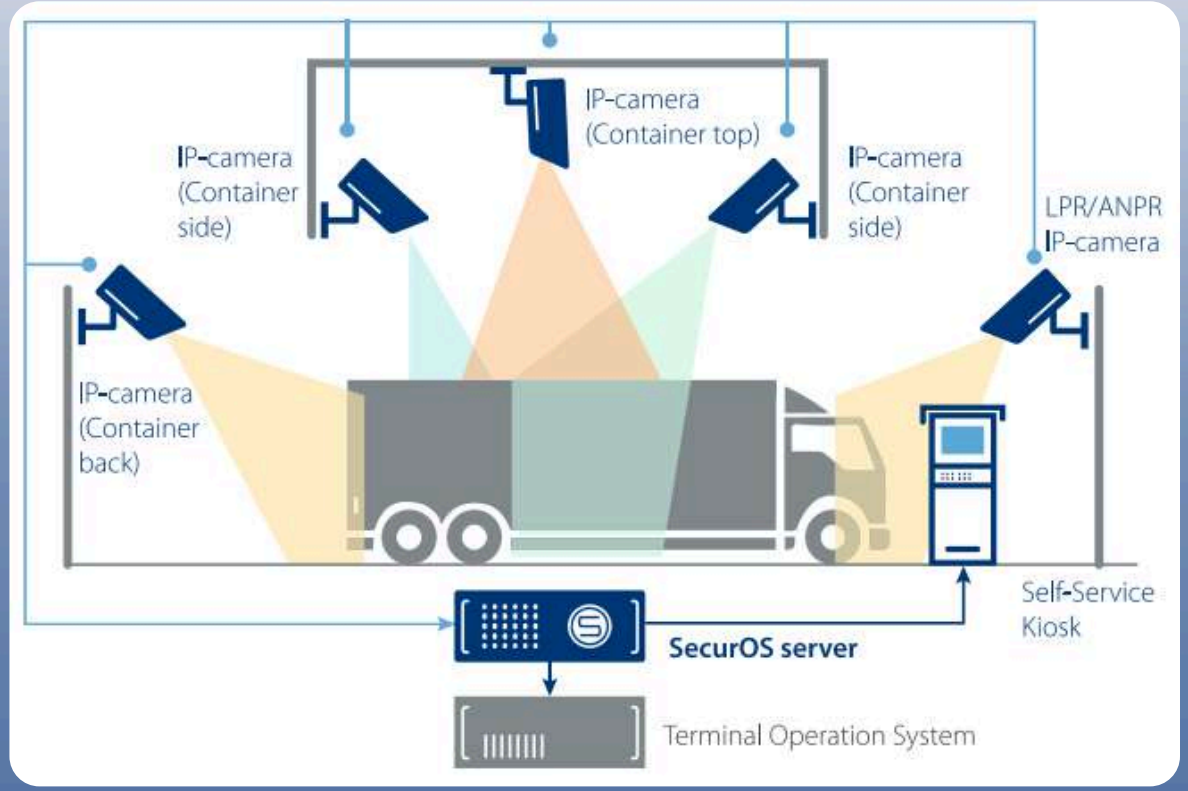
VISUAL INSPECTION AND AUTOMATION OF TERMINAK GATES SYSTEM

SecurOS Cargo Terminal

SecurOS Cargo Terminal facilitates data flow processing and seamless integration with Terminal Operation System.

This software-hardware based solution automatically collects and provides to TOS full set of Gate metadata:

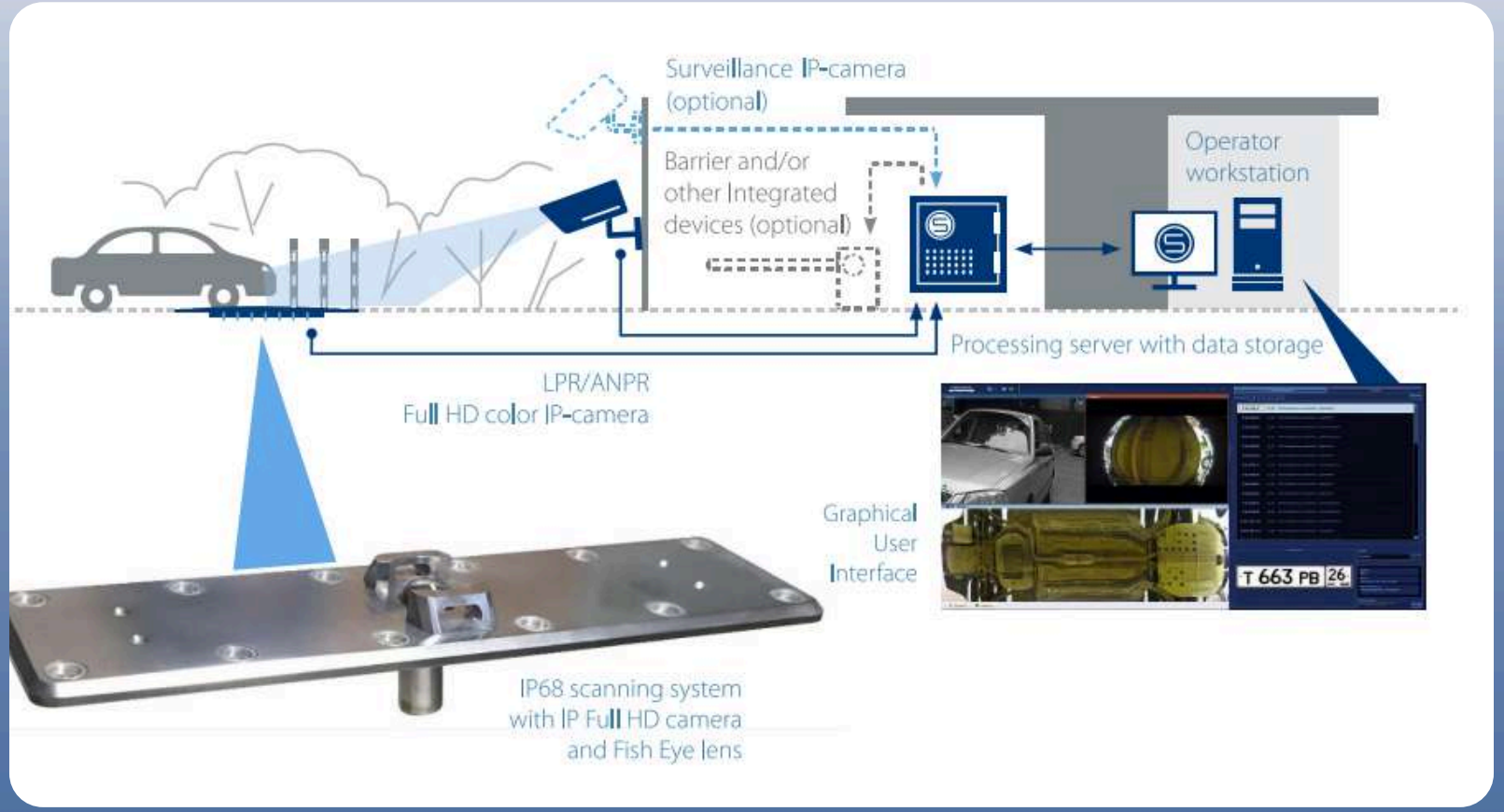
- ISO Container images for visual inspection
- ISO container number, Size and type code, Kemler, IMDG, ILU
- License plate of a truck
- RTSP video stream and ASF/AVI video clips



UNDER VEHICLE SURVEILLIANCE SYSTEM

SecurOS Flatimus

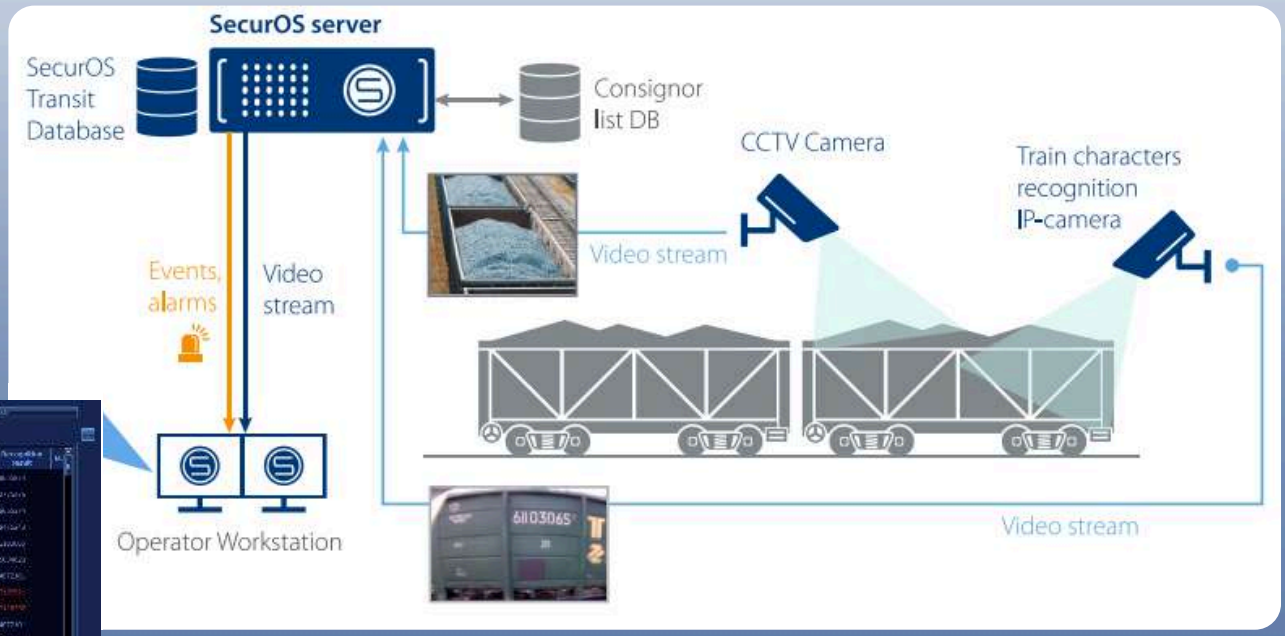
SecurOS Flatimus is a hardware-software based system of remote under-vehicle surveillance. The system creates a database of high-resolution undercarriage images and recognizes vehicle license plates.



RAILWAY CARS NUMBER RECOGNITION AND REGISTRATION

SecurOS Transit

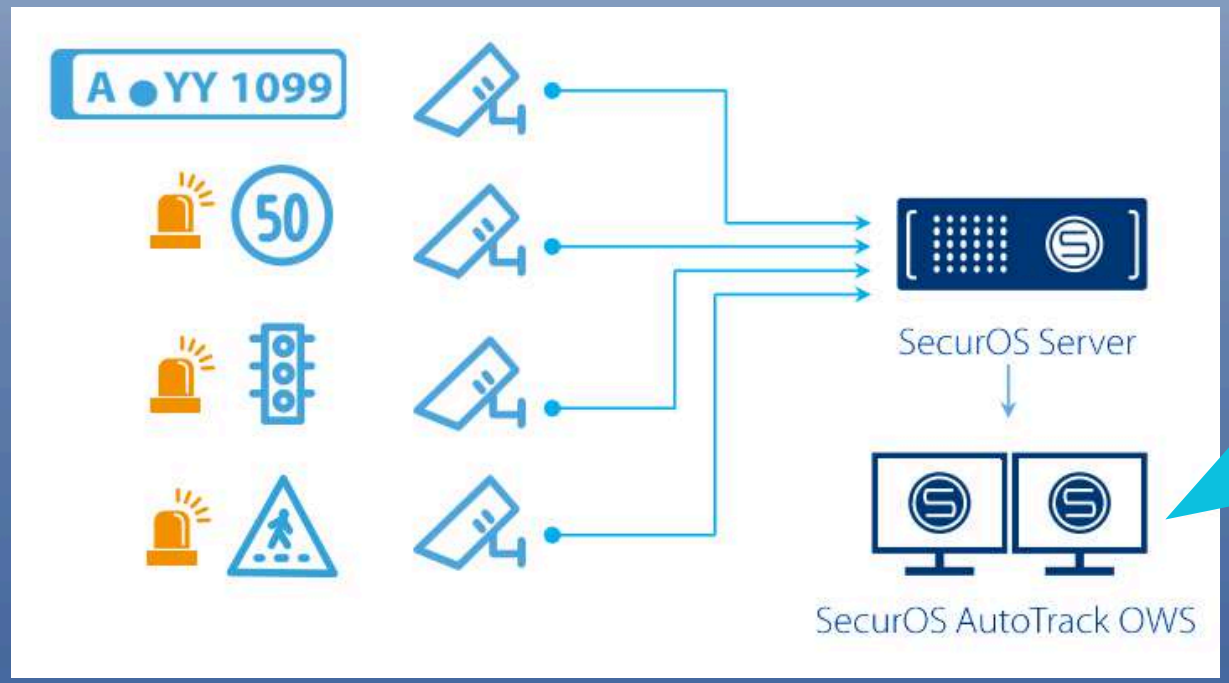
SecurOS Transit is an effective software solution for registration of train cars, tankers, and platforms at the shunting-yards, customs terminals, railroad hubs, industrial enterprises, warehouses, etc.

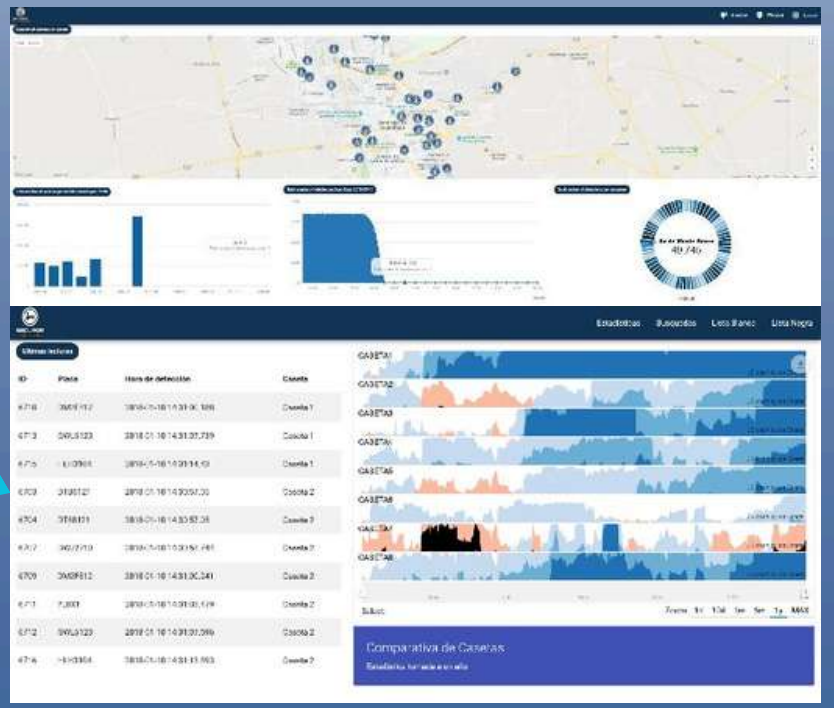


BUSINESS INTELLIGENCE FOR ITS AND LAW ENFORCEMENT

SecurOS AutoTrack

SecurOS AutoTrack is a software enables data aggregating, processing, and display of processed data in a convenient for operator form about vehicles moving on roads. SecurOS AutoTrack supports large distributed systems focused on flexibility and scalability, and provides transformation of raw data about road traffic into a suitable for business analysis form, as well as tools for shared work with such data.



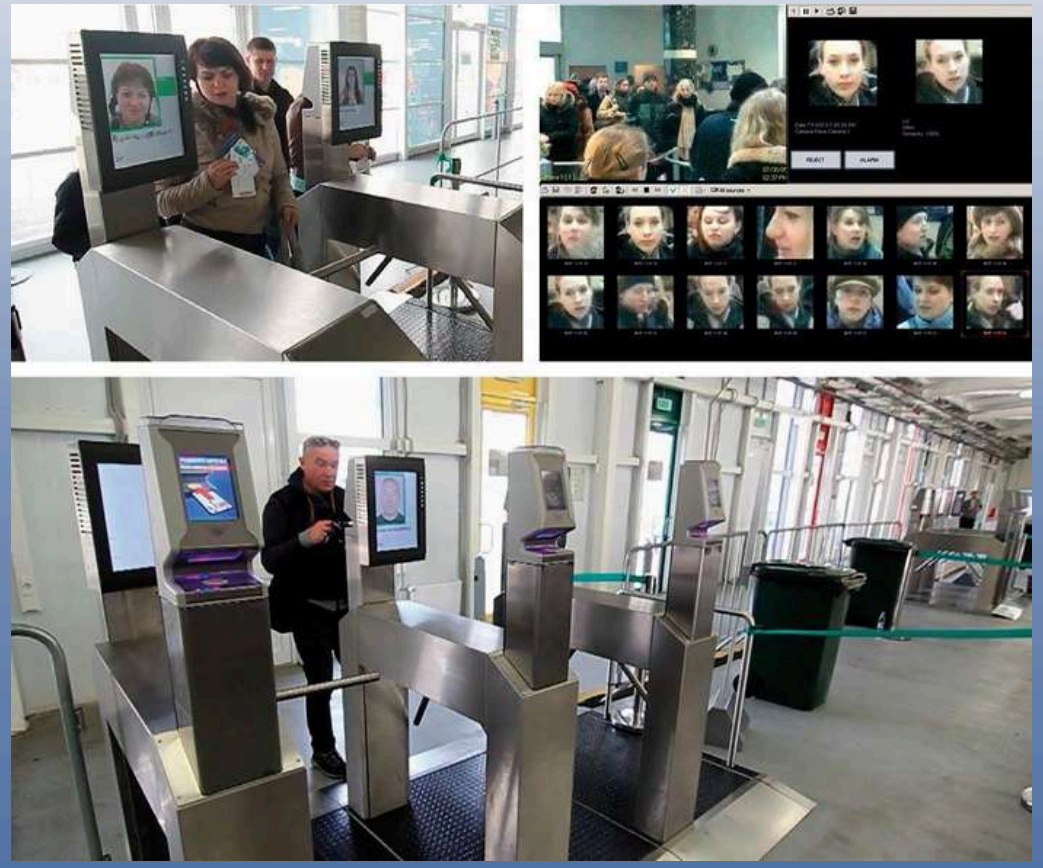


FACE CAPTURE & RECOGNITION

SecurOS Face

SecurOS FACE provides Face Capture & Recognition with a high accuracy level in a wide variety of challenging conditions and as such, is ranked among the most accurate of all Face Recognition systems in the marketplace.

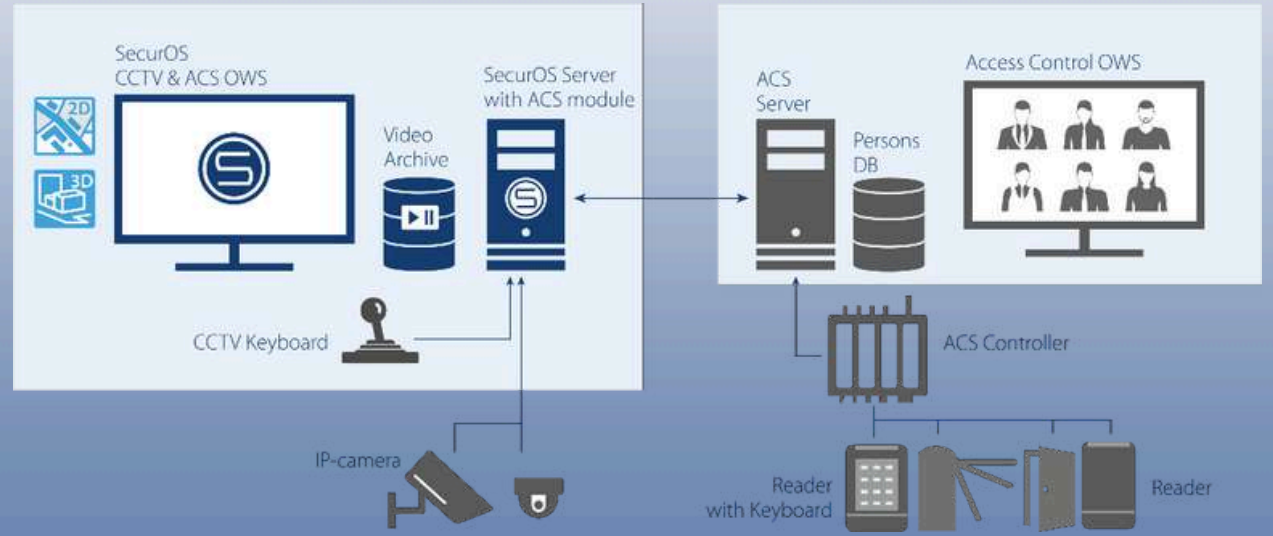
The reason of a high level of accuracy has to do with the experience of IS specialists in image analytics technology, and the related expertise with advanced algorithms, which then identifies and matches an individual's specific features with relentless attention to every detail.



ACCESS CONTROL SYSTEM

SecurOS ACS module

ISs introduces a comprehensive solution to enhance access control in high-security installations. By combining SecurOS VMS with an integrated access control system, you can create a modern, flexible and scalable system to effectively monitor staff and visitors.



SecurOS GUI Operator Workstation (OWS) is expanded with the ACS / Fire alarms operator's functionality

ACS / Fire alarms operator's functionality can be expanded with automated multi-factor authentication with video analytics: LPR/ANPR (SecurOS Auto) and face capture and recognition (SecurOS Face)

Scripting (operating scenarios) in accordance with the objectives of a particular site and ACS/Fire alarms system

POS & ATM TRANSACTION MONITORING SYSTEM

SecurOS POS

SecurOS POS is an intelligent software module of SecurOS VMS, which links live video with transaction data from a POS or ATM system. It allows search of specific transactions and review of the exact video archive of that transaction.
It provides full video documentation on selected transaction IDs, item numbers, terminal numbers, employees, customers, payment details, or stores in any combination you wish.
Effectively combat fraud and loss occurring in transactions. Integrate with other analytics to provide a complete retail solution, including recognition of known shoplifters, inventory management, after-hours surveillance, license plate recognition for gas stations, etc.

SITUATIONAL AWARENESS VIDEO ANALYTICS

SecurOS Tracking Kit III (ecurOS Computer Vision subsystem

SecurOs Tracking Kit Ill detectors provide significant reduction of operator's load: no need for constant monitoring of all control areas and exclusion of human factor influence

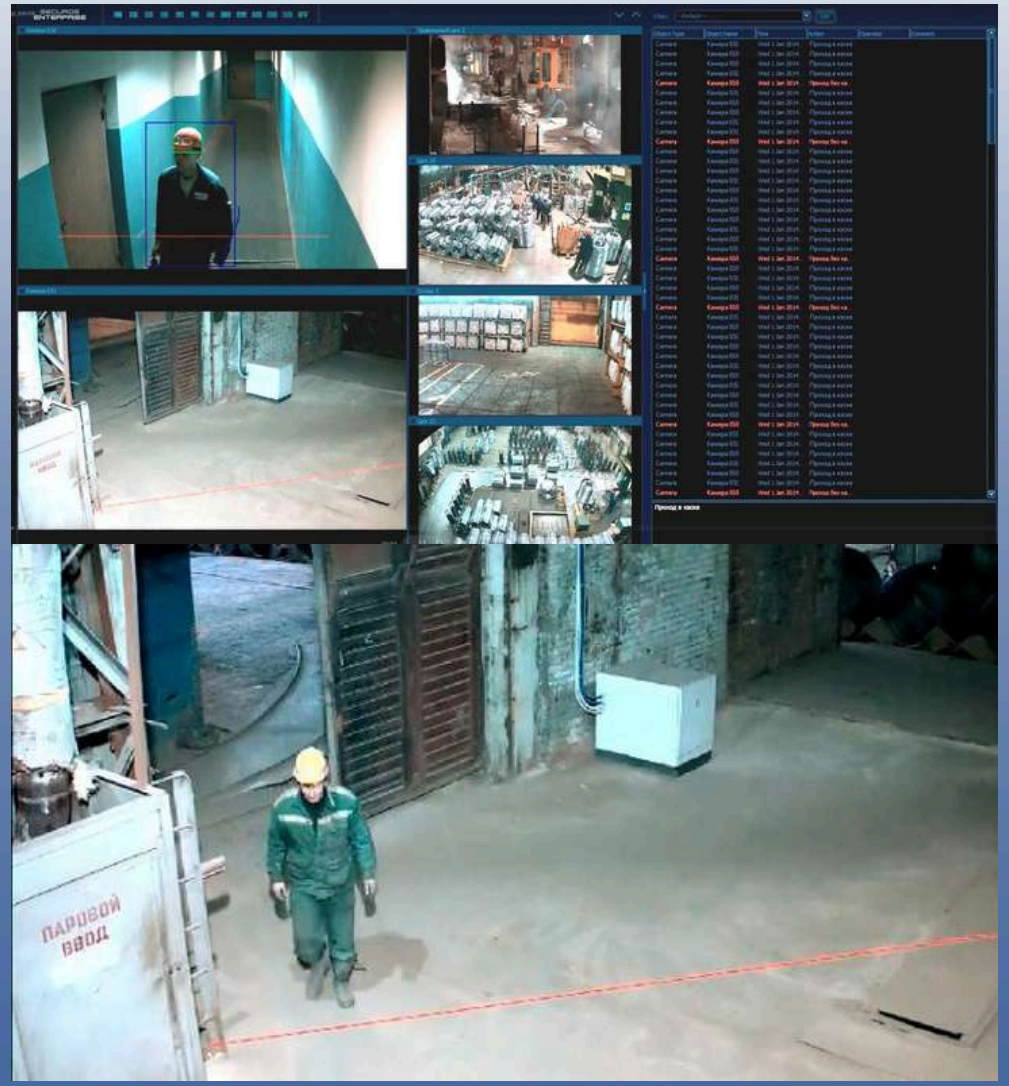
- Crowd Detector
- Loitering Detector
- Object Left Behind Detector
- Running Detector
- Dwell Time Detector
- Intrusion Detector
- Object Counter
- Line Crossing Detector
- Wrong Direction Detector
- Smoke Detector

NON-HELMET DETECTOR (VIDEO ANALYTICS)

Construction site, foundry, coal mine - work in such areas requires strict compliance staff safety rules, including using of protective equipment. One of the most frequently used tools is a helmet.

ISS video analysis, in conjunction with strategically placed video surveillance cameras, allows the detection of production staff who are not wearing protective head gear in areas where it is required

The accurate reads the video analytic systems provides, even in poor lighting or steamy conditions. The highly intelligent nature of the algorithms makes this possible, and results in very few false alerts.

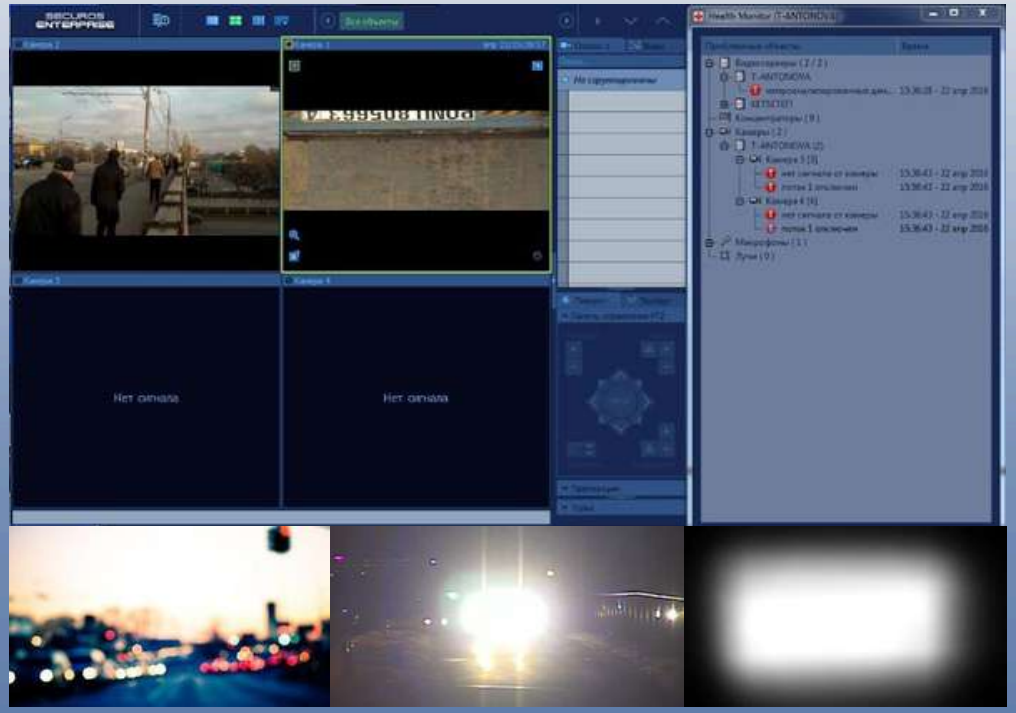


SERVICE VIDEO ANALYTICS

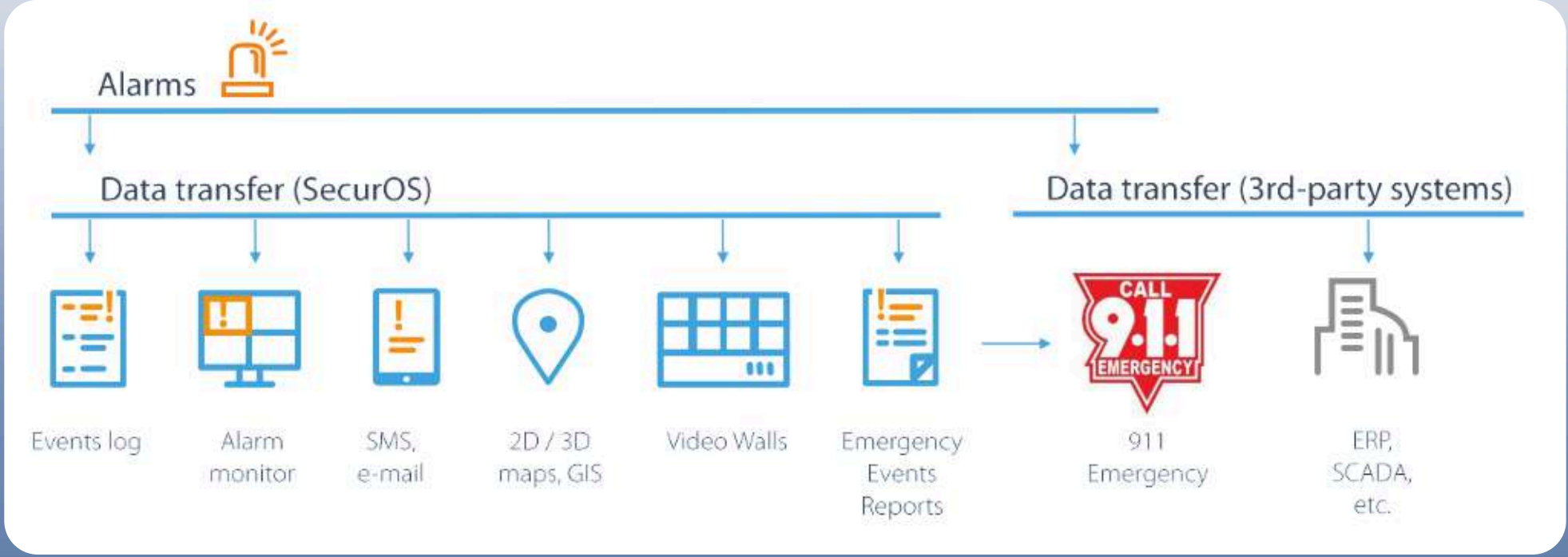
SecurOS Camera Health

Used to verify operation of the CCTV cameras and the video stream according to the technical requirements of the system and is implemented on the basis of the service detectors

- **Loss of signal** from the camera logs communication blackout between server and camera
- **Defocusing** responses in case of the image sharoness loss
- **Blinding** registers light beam directed at the lens.
- **Camera shielding** reacts to the darkening of the image in cases of closure of lens, failure of the lighting device
- **Changes the field of view** registers unauthorized rotates of the camera



EVENT MANAGEMENT

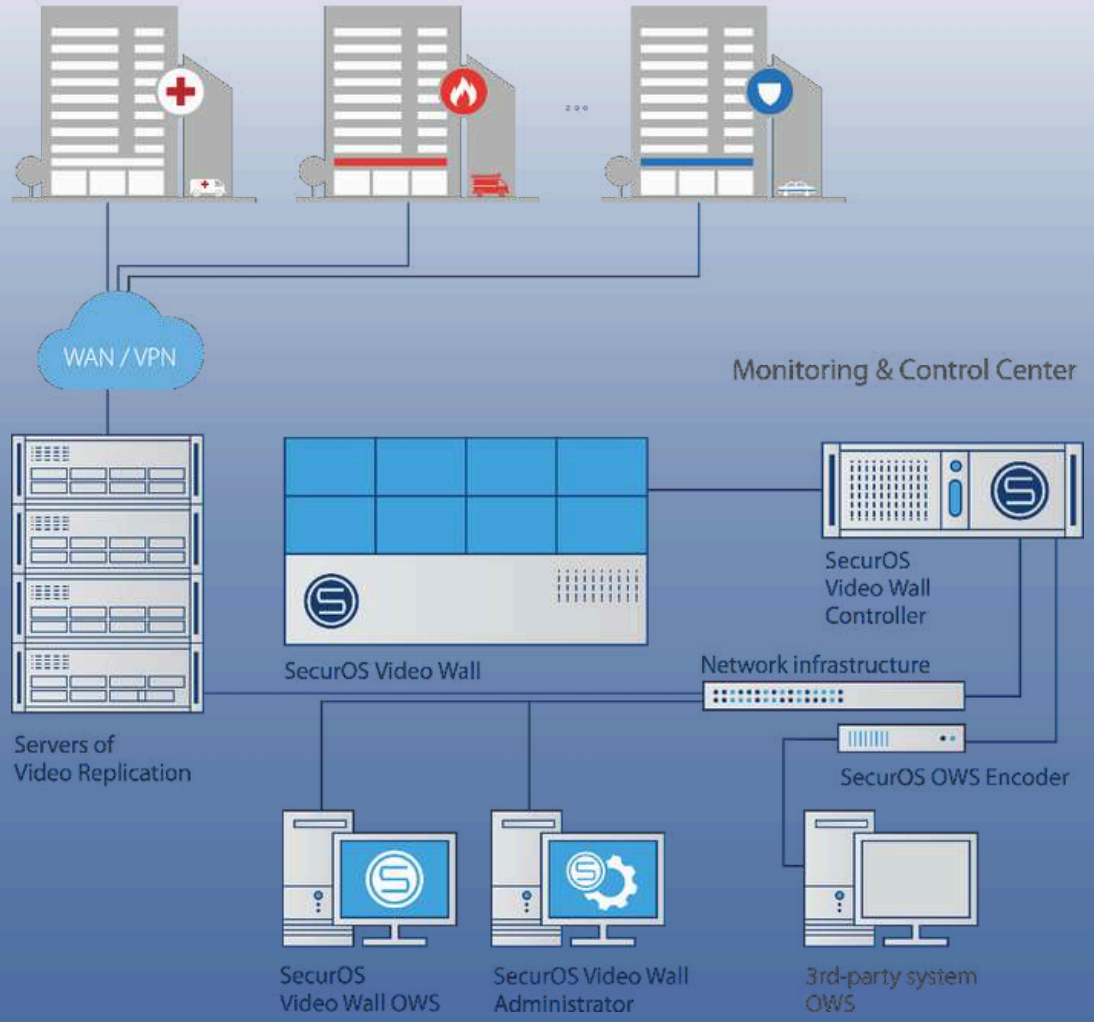


ISS advanced integration capabilities allow to develop integrated solutions based on video management platform, including a number of additional subsystems (video analytics, event processing, GIS, "91 1", etc.) and hardware (terminals "Citizen-Police", acoustic, chemical and radiation sensors, systems, Fire Alarm, etc.).

MONITORIING & CONTROL CENTER

SecurOS MCC

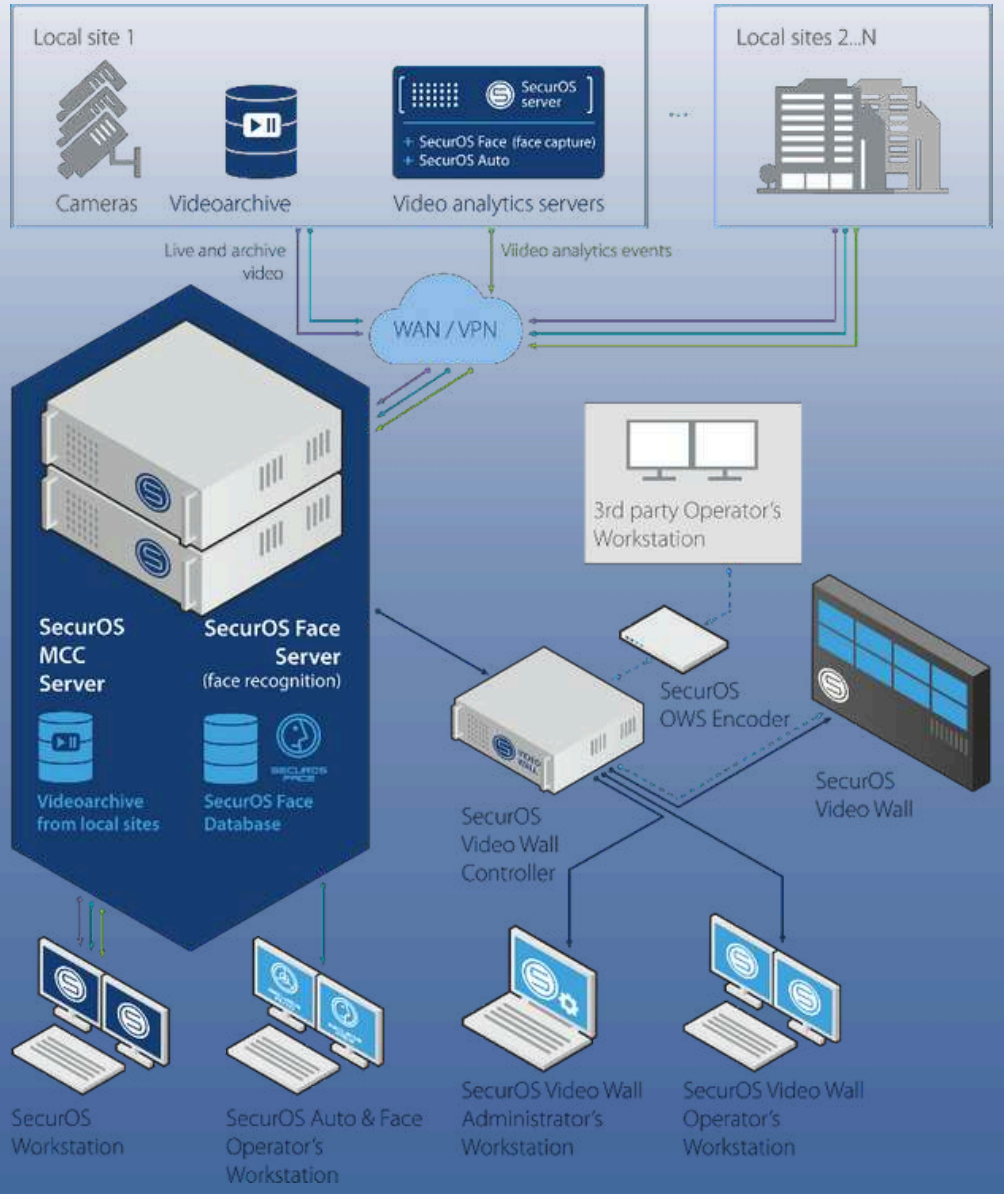
SecurOS MCC provides the global monitoring and management of a complete remoted security infrastructure of all your local sites (as if they were part of a single virtual system) from a single command center. It is an excellent solution for customers with multiple geographical disparate sites or business facilities located at vast area.
SecurOS MCC allows for a much more streamlined workflow and globalizes security operations to make security personnel more productive and better informed.



MONITORIING & CONTROL CENTER

SecurOS MCC

The SecurOS MCC federation capability scales as needed to tie together a few sites to hundreds and thousands of globally disparate sites, and provides management of all SecurOS servers within the virtual network and visualization of all cameras and other devices which are connected to each individual SecurOs deployment.
The flexible SecurOS architecture allows to create a hierarchical structure from several Monitoring & Control Centers. One MCC can be top-level to others MCC-s or the responsibilities can be divided among a number of MCC-s in accordance with customer's needs.



VIDEO WALL

SecurOS IVS VideoWall

The SecurOS MCC federation capability scales as needed to tie together a few sites to hundreds and thousands of globally disparate sites, and provides management of all SecurOS servers within the virtual network and visualization of all cameras and other devices which are connected to each individual SecurOs deployment.
The flexible SecurOS architecture allows to create a hierarchical structure from several Monitoring & Control Centers. One MCC can be top-level to others MCC-s or the responsibilities can be divided among a number of MCC-s in accordance with customer's needs.

MOBILE APPLICATION FOR IOS AND ANDROID DEVICES

SecurOS Mobile

SecurOS Mobile is a mobile client for Securos MS which gives security personnel capabilities to monitor video and control cameras on their mobile phones and tablets (iOS and Android). Operators can easily access live video streams, playback video archive, monitor video analytics events and other types of alarms over Wi-Fi or 3G/4G networks.
Set up access and save credentials for multiple SecurOS systems
SecurOS Mobile can be download on the App Store and the Google Play

Set Up access and save credentials for multiple SecurOS systems

Review alarms

Playback up to 4 cameras simultaneously in various speed


TACTICAL SIMULATION

ADVANCED VR MILITARY SIMULATION SOFTWARE

GTS software enhances land forces' training and preparedness by combining immersive, realistic environments with flexible, instructor-controlled scenarios and robust group training capabilities. It integrates realistic hardware like haptic feedback devices, motion tracking systems, and weapon simulators, providing tactile and immersive interactions. This realism helps trainees develop muscle memory and operational proficiency, ensuring a seamless transition from virtual training to real-world operations.

IWS

The Instructor Work Station provides comprehensive tools for real-time scenario control, performance monitoring, and detailed analytics, empowering instructors to deliver highly effective training sessions.

Data Analysis

The system's advanced data analysis capabilities track and evaluate trainee performance in real-time, providing detailed reports and insights into individual and team effectiveness. This data-driven approach allows instructorsto identify strengths and areas for improvement, ensuring that training is both efficient and targeted.

Group Training

One of the standout features of our VR military simulation software is its robust support for group training. This capability ensures that entire units can train together in a cohesive and coordinated manner, replicating real-world team dynamics and operational scenarios.

Muscle Memory

The realistic hardware integration, including haptic west, helmet devices and weapon simulators, enhances muscle memory development, ensuring trainees can seamlessly transit from virtual training to real-world operations.

Realistic Hardware Integration

To enhance the immersive experience, our software integrates a realistic hardware that replicates the physical sensations and interactions of real-world operations.

GTS SOFTWARE: SAVINGS IN TRAINING, STRENGTH

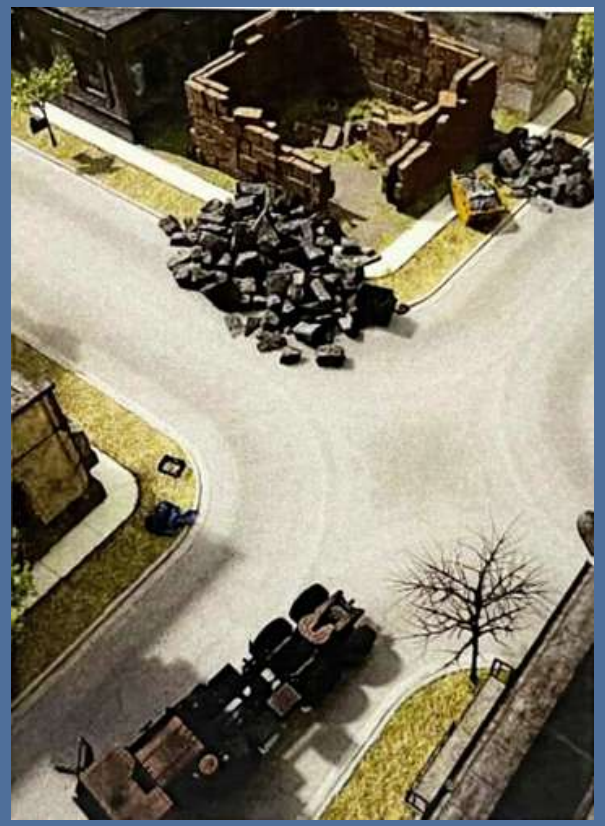
VR MILITARY TRAINING SYSTEM (GTS) FROM INFINIT SIMULATION

Power data with AI

The system records and analyzes trainee data througout their career, providing unique tactical performance insgihts. This identifies weak skills for targeted improvement and challenges top performers with complex scenarios. It smooths out skill differences, allowing for effective specialization. AI-driven analyses optimize team compositions and training methodologies, enhancing overall effectiveness.

Implementation

GTS is vital for enhancing skills and survival chances. Broad GTS implementation will ensure realistic and comprehensive training for a more lethal and resilient force.



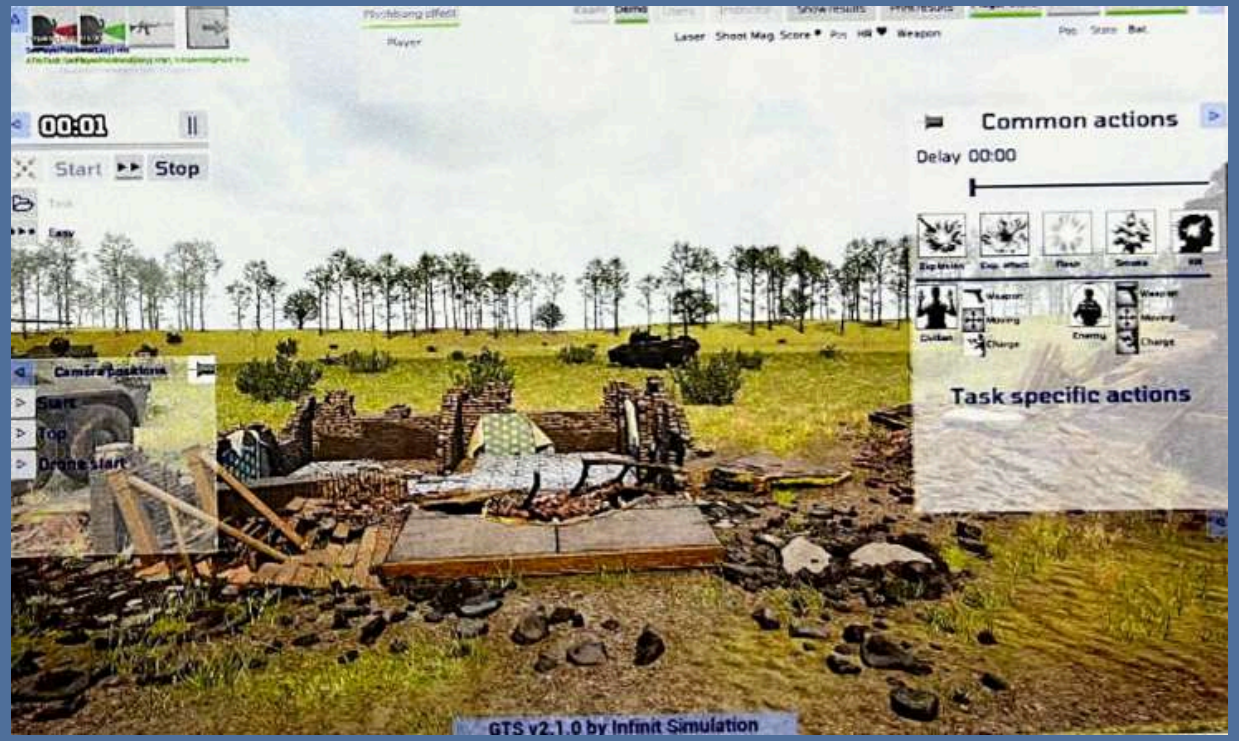
Lessons Learned and Preparations

Scalable and customizable, our solution quickly adopts to specific needs, such as mission reharsals.

INSTRUCTOR WORK STATION (IWS)

The IWS is a central hub for managing training session.

- Real time monitoring
- Comprehensie Analytics
- Scenario Customization
- Communication Integration



GROUP TRAINING CAPABILITIES

GTS supports synchronized training for entire units, allowing coordinated team exercises in realistic virtual environments. This tosters ettective communication, teamwork, and tactical proficiency.

ZERO-LEARNING-CURVE

Trainees use I: weapon replicas with realistic handling and safety procedures. ThIS ensures muscle memory development, similar to live shooting practice. The system IS intuitive, requiring no additional coaching for those without computer skills.

TRAIN AS YOU FIGHT -REAL LIFE SKILLS

GTS immerses trainees in realistic environments, replicating real-life combat stress. Soldiers under simulated enemy fire show elevated heart rates and cognitive regression. Practicing in this environment improves performance, making skills transferable to real-world situations. This cost-effective approach benefits both new recruits and elite warriors.

COST SAVING

Unlock savings with our comprehensive training plan, cutting ammunition costs by up to $31,000 per individual soldier, (amounting to $12,400,000 annually for 400 reserve soldiers training). Implementing the full training plan from individual to squad level saves $162,087 per squadron per cycle, (totaling $1,458,00 yearly for a single infantry company's squads). Achieve substantial reductions with items like the $3,000 Carl Gustaf missile, while also benefiting from decreased weapon amortization, logistics, and other costs.

UNDER DEVELOPMENT

Our VR system is expanding to include simulations for advanced vehicles such as helicopters and tanks. This will allow trainees to practice piloting and operating these vehicles in realistic combat scenarios. The integration of these vehicles will further enhance the breadth and depth of our military training solutions.

GTS HARDWARES

Our custom-designed hardware technology, including haptic vests, helmets, and weapon simulators, offers unparalleled realism by providing tactile feedback that mimics real-world interactions. This advanced hardware integration ensures that trainees develop accurate muscle memory, enhancing their readiness and proficiency in actual combat situations. By seamlessly blending physical sensations with virtual environments, our technology creates an immersive training experience that is both engaging and highly effective.

Circuit system
Our custom circuit system ensures seamless and precise integration of all hardware components for optimal performance.

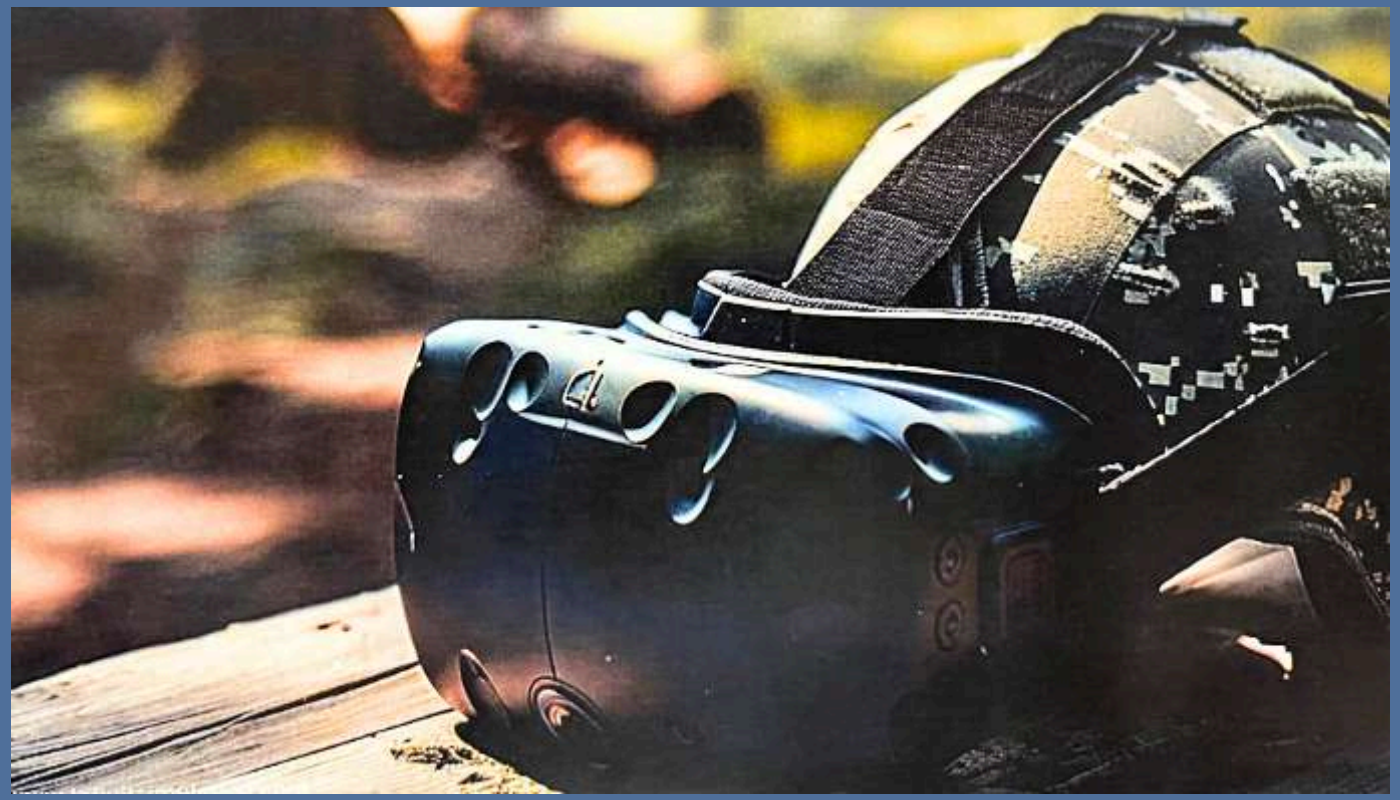
Realistic recoil system
The realistic recoil system provides authentic feedback, simulating the true feel of firing a weapon.

Realistic magazine change
This feature ensures trainees experience authentic weapon handling and reloading during simulations.

Realistic fire selector switch system
The realistic fire selector switch system accurately replicates the functionality of real-world weapon modes.

HELMET

Our custom-designed helmet is equipped with advanced sensors, providing a highly immersive training experience by simulating realistic head movements and impacts. Integrated with our VR system, the helmet offers a wide field of view, high-resolution display, and built-in headphones with realistic 3D sound, ensuring trainees can engage with the virtual environment with unpar- alleled clarity and realism. This innovative design enhances situational awareness and contributes to the development of critical skills needed for real-world operations.

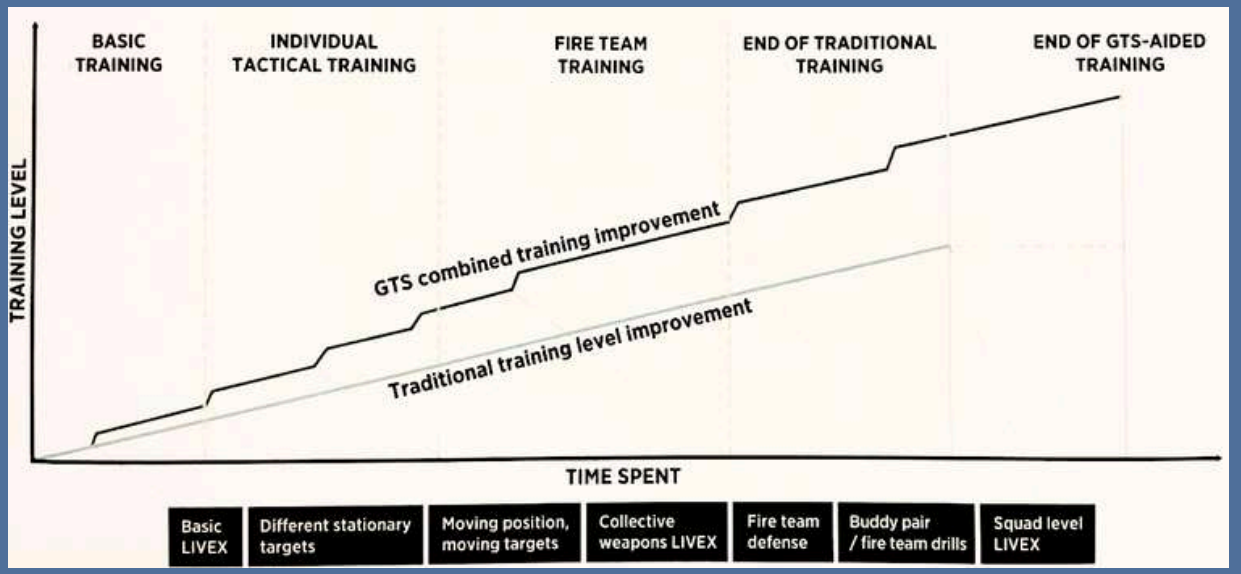


ADVANTAGES COMPARED TO COMPETITORS

Interactive simulation systems are partly determined by the technology used, but the software that runs gives the greatest competitive advantage. Testing and monitoring the competition shows that our system is much more complex, better thought out and much more extensible which is a result of the combination of 7 years of VR development experience and 10+ years of military training research and development.

	Infinit Simulation	Other VR based platforms	AR based platforms	Laser based platforms
Continuous technical updates	✓	✓	✓	✓
Perfectly tailored to the needs of the costumer	✓	✓	✓	✗
Biometric sensor integration	✓	✗	✗	✓
Customizable haptic feedback	✓	✗	✗	✗
No training room setup needed	✓	✓	✗	✗
Unlimited variety of scenarios	✓	✓	✗	✗
No nausea	✓	✓	✗	✓
IWS with instant AI backed data	✓	✓	✗	✗
No need of heavy, special equipment	✓	✓	✓	✗
Cutting edge graphics	✓	✗	✗	✗
From basic training to complex combined-arms training	✓	✗	✓	✗
Complex tactical situations with all inputs	✓	✗	✗	✗
Easy to deploy	✓	✓	✗	✗

KNOWLEDGE LEVEL CHANGE WITH GTS



This chart presents the training cycle from the basic training up to the squad-level live firing exercise (LIVEX) with the shooting and tactical training in focus. On the chart, a blue line marks the training level achieved with the traditional training procedures. The green line marks the achievable training level with the help of the GTS. The chart's data is based on our scientific research which according to with 25% more time of training (that time is solemnly allocated to the GTS) up to 58% higher training level can be achieved at an average. The whole training cycle begins with the basic training. It is followed by individual tactical training, collective weapons training, and subsequently the fire team and squad-level training phases. In each phase, even more complex and dangerous LIVEXs are executed. With the help of the GTS, the soldiers will accomplish these tasks more safely and more efficiently than before. The reason behind this advancement is that with the help of the GTS, the soldiers can deepen their knowledge in the areas of safe weapon handling, the coordination of fire and maneuver, and organizing a system of fires of different weapons. Further- more, the soldiers can do so in a diverse and immersive environment. Therefore, before each LIVEX, the soldiers will obtain deep knowledge and they will build an accurate muscle memory with all the good practices based on which they will execute the LIVEs more safely and at the same time, far better results.

THANK YOU