Oyamo Group

Oyamo Group Proposal for Defensive and Offensive Cyber System

Cyber Intelligence & HLS

HLS and Crisis Management main Pillars

- **Powerful Command and Control**
- **Fixed / Deployed and On the Move**
- **Networked Command Centers**
- **Scalable Emergency Communication**

Networked Command Centers

The **Networked Command Centers** Solution interconnects the **National level** Command Centers with the **Regional /Local** Command Centers and **Tactical Forces**, in execution of the **C5I2SR integrated** process

National/ Joint Level Headquarter

Regional / Local Level Headquarter

Mobile Headquarter

Integrated C5I2SR Application

ROIP, VOIP & Communication Means: Fixed, Deployed & on-the Move links upper/Lower echelon, V/U/HF, VSAT/SOTM

All communication types –Full connectivity & integration

Operational / Tactical Units control

National /Regional/ Local/Tactical Infrastructures open Interface

Secure Mission-Critical Services

Scalable Emergency Communication

Secure immediate communication using cellular network

The system is a leading Mission Critical PTT Communication solution for Secured mobile voice and multimedia services for Government agencies, special units and various emergency forces.

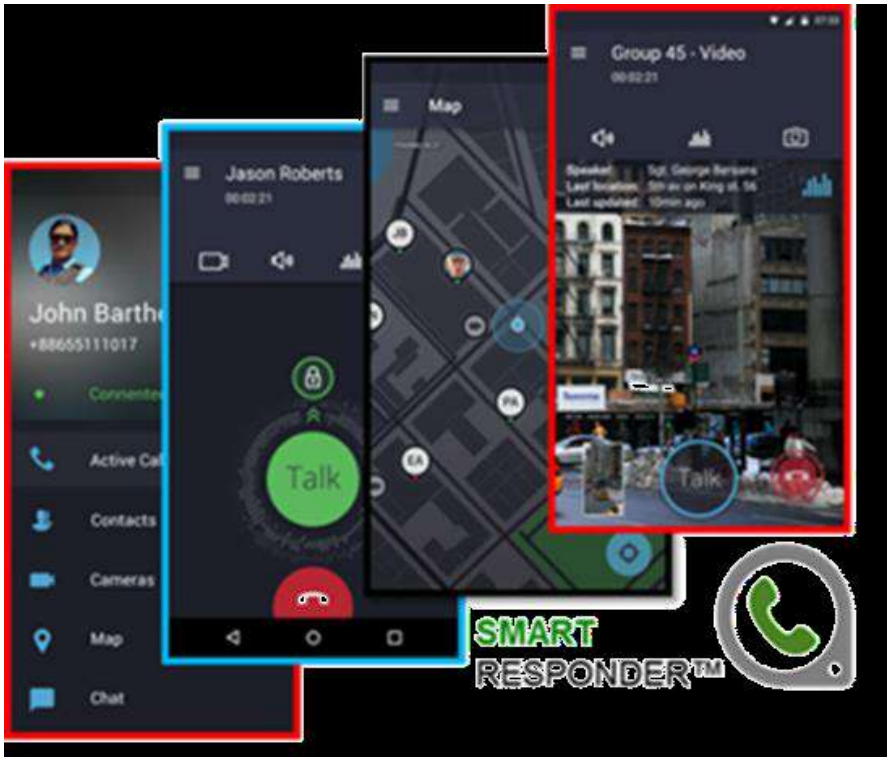
SOLUTION OUTLINE

The system is a secure, cloud-based unified communications suite that provides the basis of an ecosystem for real-time voice, video, and data sharing services with voice interoperability between

P25 / Tetra Land Mobile Radio and LTE (Long Term Evolution) network systems users to enhance situational awareness and operational utility. Wide Bridge supports user authentication, authorization, monitoring and management, enabling secured communications and collaboration to help law enforcement personnel execute their missions and keep themselves safer at the same time.
In order to be sure that the latest available capabilities can be incorporated into Wide Bridge, we have aligned with the evolving 3GPP (Third Generation Partnership Project), an international standards organization for the advancement of LTE. This standard defines the Mission Critical Push-to-Talk (MCPTT) design we have built on to offer enhanced communication and collaboration between law enforcement, public safety, and related agency personnel and the public to significantly enhance communications in the field and in the office. Designed with end-to-end cyber security mechanisms baked-in, Wide Bridge empowers law enforcement users' capabilities and tools that push existing boundaries of limited voice communications alone.

THE SYSTEM SOLUTION CAPABILITIES

The advent of secure broadband voice, video, and data services will form the foundation of next generation public safety communications tools and capabilities to come.
Wide Bridge platform meets most recent standards made for Public Safety broadband communication – the Mission Critical Push to Talk (MCPTT) standard.



The system is a set of public safety Telco-grade, converged, secure broadband Software platform to deliver:

Voice & Video point to point calls (full duplex)

Push-To-Talk (PTT) group calls

Push-To-Video (PTV) group calls “see what I see”

Video streaming from network cameras

User’s presence and status

Location based services

LMR (TETRA) - LTE Voice interoperability

All traffic is AES-256 encrypted end to end

PTT/PTV group media recording

System Communication Stations for HQ’s

Independent 4G Network Deployed cell

The system has been developed using key technologies deployed in some of the most demanding environments in the world. We employ a partner ecosystem consisting of known and trusted providers to commercial carriers, to deliver IMS, SBC, SDP, MRF, and other core services.

SYSTEM SOLUTION

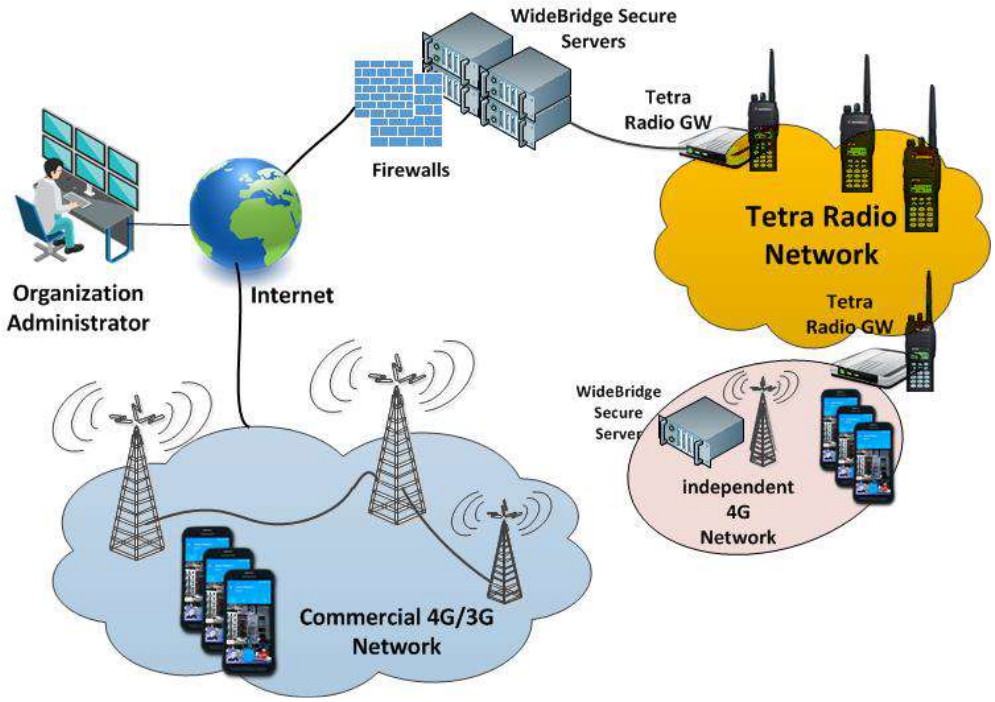
- To provide secured mobile voice and multimedia services for Government and Special Forces, the system solution offers an innovative communication concept for extending voice, video, and data.

The proposed solution offers:

- Maximize the utility of the broadband network to provide first responders new tools and capabilities available nationwide, anytime.
- Enable Voice interoperability with existed TETRA LMR networks (Optional capability).
- Provide Interoperability between different organizations (first responders) and communication network solutions. Administration system enables communication between different

organization by connection to common voice/video PTT groups, information sharing and common operation picture management.

- Enable seamless mobility and operation in different terrains and environments (Urban, Rural and Subterranean).
- The Figure below describes the system architecture:



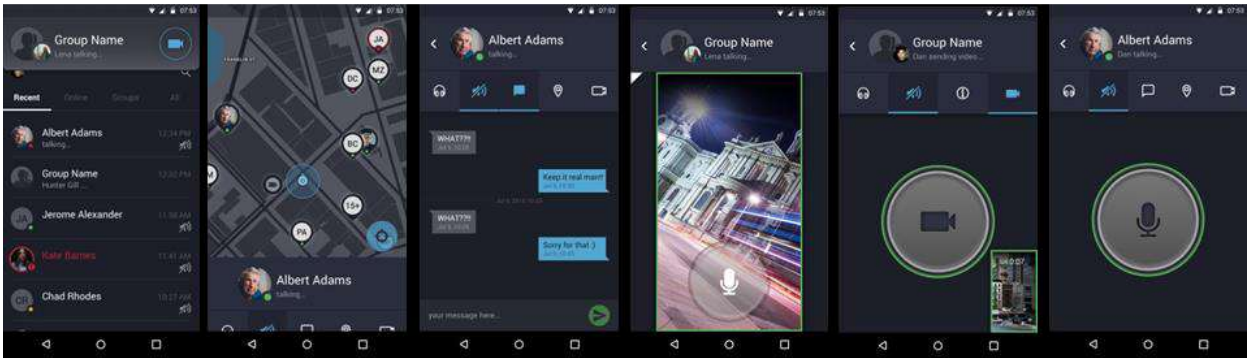
The solution presents a concept of

- End-to-end secured and encrypted multimedia services for government agencies and offices (voice, video and data) while using the pubic cellular infrastructure
- Immediate and direct communication for all personnel
- Voice connectivity to Radio Networks

The proposed solution uses commercial cellular network (Using the pubic cellular infrastructure) to provide End-to-end secured and encrypted advance multimedia services for government (voice, video and data)

MOBILE DEVICE APPLICATION

Wide Bridge is an intuitive SIP based application with high audio quality and it is easy to setup on many devices including smartphones and tablets. It works flawlessly in the background and is optimized to consume low power while ensuring the reliability of incoming calls.



The system application offers advanced security encryption, including TLS for the SIP signaling and SRTP for media which allows the user to make secured crystal clear voice and video calls over any 3G, LTE, Wi-Fi connectivity.

Major system capabilities of the system application are described below:

- Voice Call – Secured full duplex voice call
- Video Call – Secured full duplex video call
- Push to Talk (MC-PTT) Group Voice services (half duplex with floor control)
- Push to Video (MC-PTV) Group Video Services: Picture and video packets' distribution, enabling users to send or receive video (half duplex with floor control).
- Presence: Active stations contact acquisition and display.
- Location based services: current location of all active users over digital maps, using smartphone's internal GPS receiver.
- Dynamic address book – Use a dynamic address book to locate the members you want to talk with
- Active Speaker – Identify the active speaker on each one of the active calls
- Security – A secure Real-Time Transport protocol provides AES-256 encryption and message authentication and replay protection of the RTP data in unicast and multicast, including SIP signaling transport.
- Secured Streaming Video – Video streaming from video sources (IP cameras linked to the cellular network). A secured connection with the Video Distribution Server to stream backs the video source signal (optional).

The system is supported on a large portfolio of devices. Here are some examples:



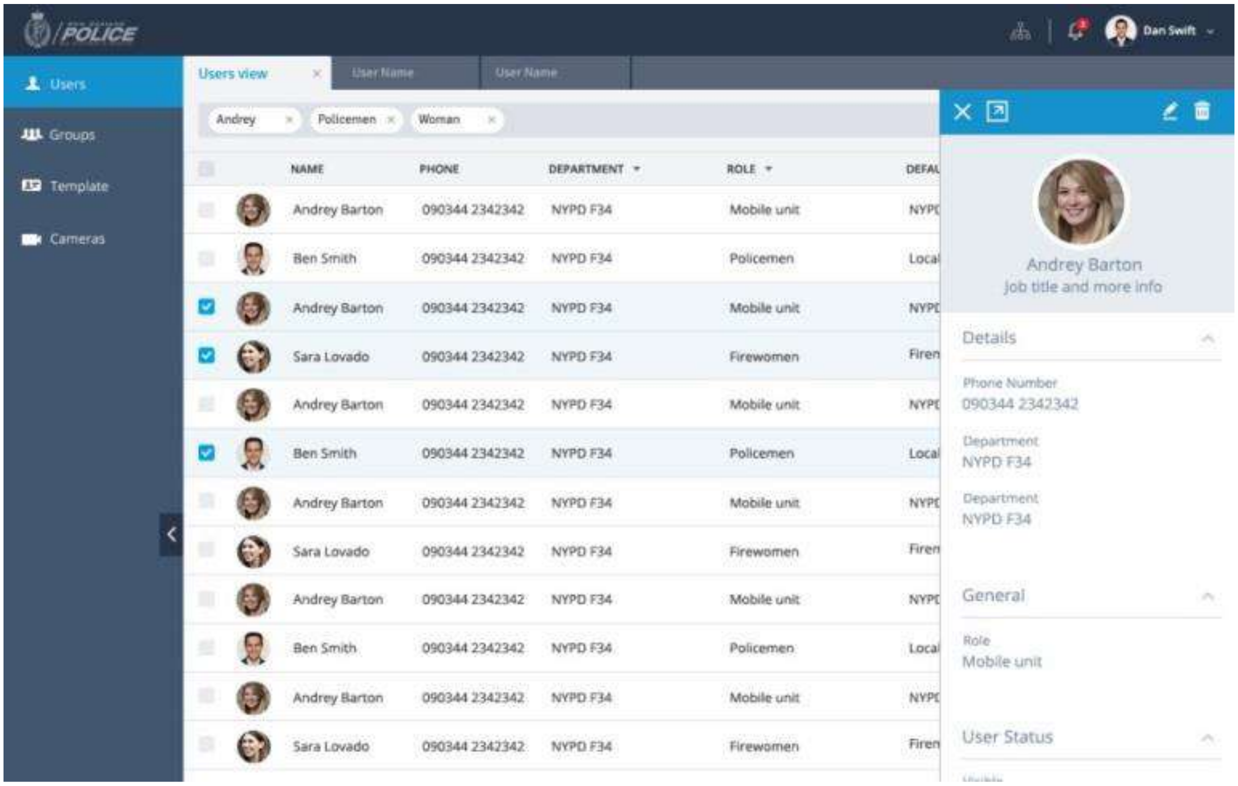
SYSTEM PROVISIONING - ADMIN TOOL

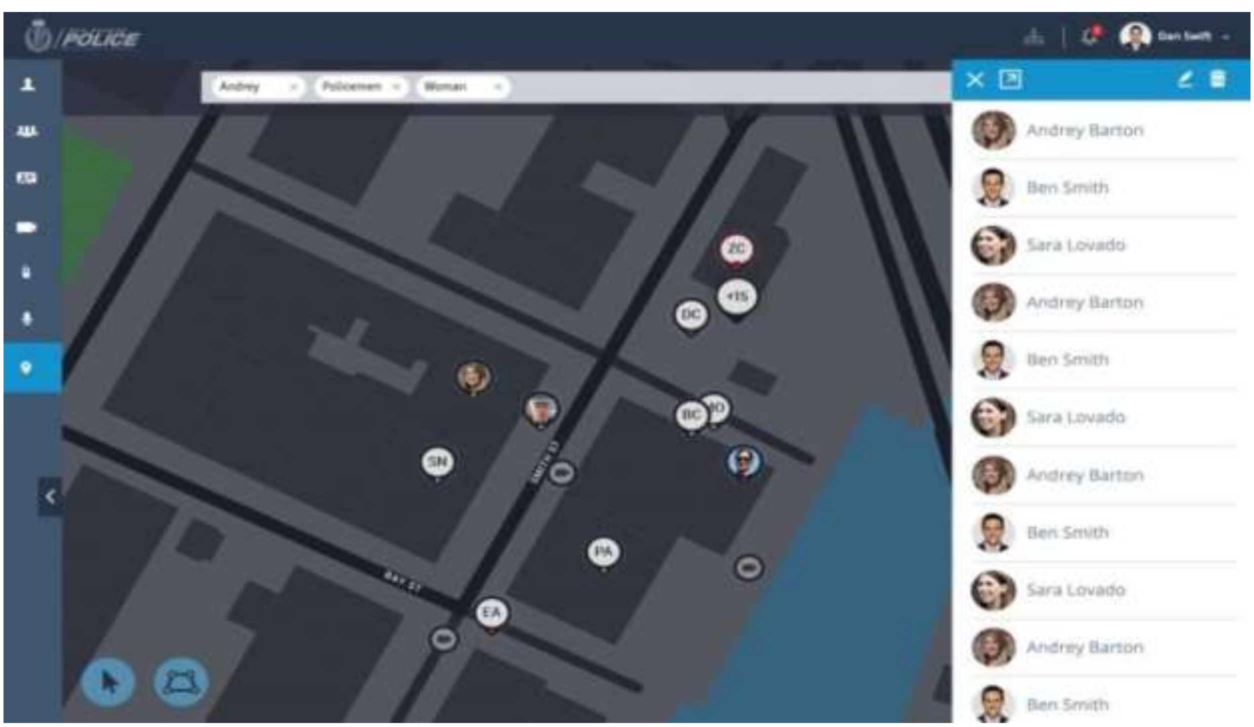
Administration tool is a Web based application for administrators. The App includes Wide Bridge Set Up, organizations, groups and users setup.
Some of the key capabilities include:

- Agency administrator – Permission to manage his organization.
- Agency administrator – create geo-fencing groups or selective team groups, merge and extract groups based on real time missions

Admin tool general functionalities:

- Create, Update, Read, Delete of users in the system
- Create, Update, Read, Delete of groups in the system
- Create, Update, Read, Delete of organizations in the system
- Create, Update, Read, Delete of roles in the system
- Permission management per user/role/group and organizations
- General system parameters management


POLICE
Dan Swift
Users
Groups
Template
Cameras
Users view
User Name
User Name
Andrey
Policemen
Woman
NAME
PHONE
DEPARTMENT
ROLE
Andrey Barton 090344 2342342 NYPD F34 Mobile unit
Ben Smith 090344 2342342 NYPD F34 Policemen
Andrey Barton 090344 2342342 NYPD F34 Mobile unit
Sara Lovado 090344 2342342 NYPD F34 Firewomen
Andrey Barton 090344 2342342 NYPD F34 Mobile unit
Ben Smith 090344 2342342 NYPD F34 Policemen
Andrey Barton 090344 2342342 NYPD F34 Mobile unit
Sara Lovado 090344 2342342 NYPD F34 Firewomen
Andrey Barton 090344 2342342 NYPD F34 Mobile unit
Ben Smith 090344 2342342 NYPD F34 Policemen
Andrey Barton 090344 2342342 NYPD F34 Mobile unit
Sara Lovado 090344 2342342 NYPD F34 Firewomen
Andrey Barton
Job title and more info
Details
Phone Number
090344 2342342
Department
NYPD F34
Department
NYPD F34
General
Role
Mobile unit
User Status


POLICE
Andrey
Policemen
Woman
ZC
+15
DC
BC
SN
PA
EA
Andrey Barton
Ben Smith
Sara Lovado
Andrey Barton
Ben Smith
Sara Lovado
Andrey Barton
Ben Smith
Sara Lovado
Andrey Barton
Ben Smith

SYSTEM SERVERS - HARDWARE

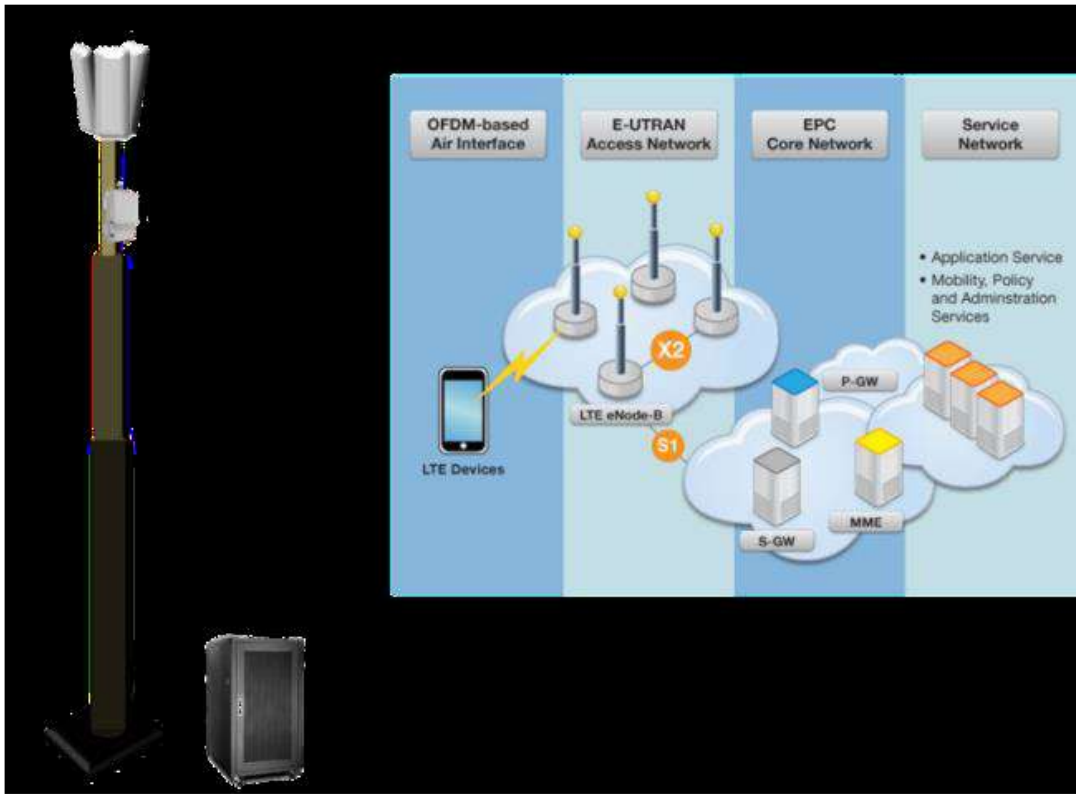
The system servers include the most advanced IT platforms, hosted in 19” rack cabin.

SITE REQUIERMENTS

The system server’s site shall be provided by the customer and shall include an air-conditioned room equipped with 220V/50Hz 32A power supply, and a proper UPS to back-up these servers for 1 hour. The site requires 100Mbps symmetrical internet connection with 16 fixed IP addresses. This also will be provided as CFE.

INDEPENDENT 4G NETWORK

In the case that the area of operation is not covered reliably by the local cellular network we propose an autonomous LTE base station; The base station contains all required components to provide up to 5 Km of LTE network coverage.



The autonomous LTE base station's components are as follow:

- 3 x Sectorial antennas 1200
- 15m Deployed Mast
- **eNodeB** or **E-UTRAN** hardware which is connected to the mobile phone network that communicates directly wirelessly with mobile handsets (UE). The eNodeB contains the Radio Network Controller (RNC).
- **EPC** (Evolved Packet Core) –core network

Operational challenge

Making the Command Center Proactive, Predictive & Preventive

PREDICTIVE

To extract intelligent info, context-dependent and alerting on potential threat

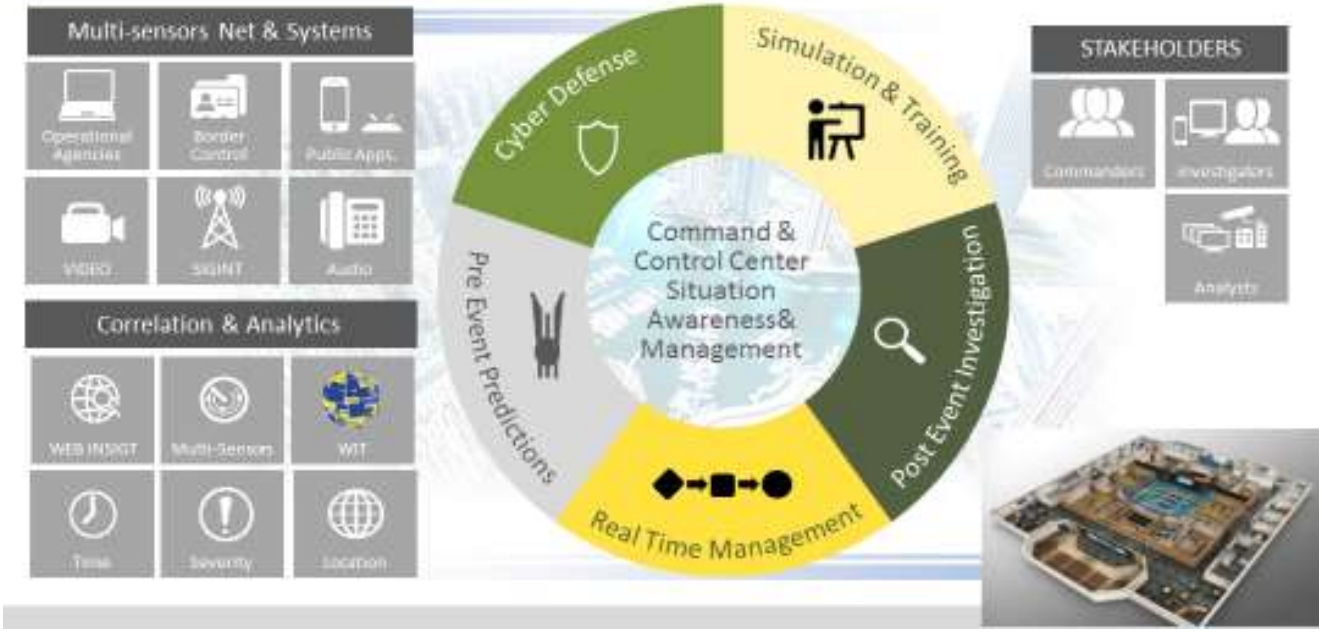
PROACTIVE

To coordinate and control all security operations between all low enforcements forces and agencies

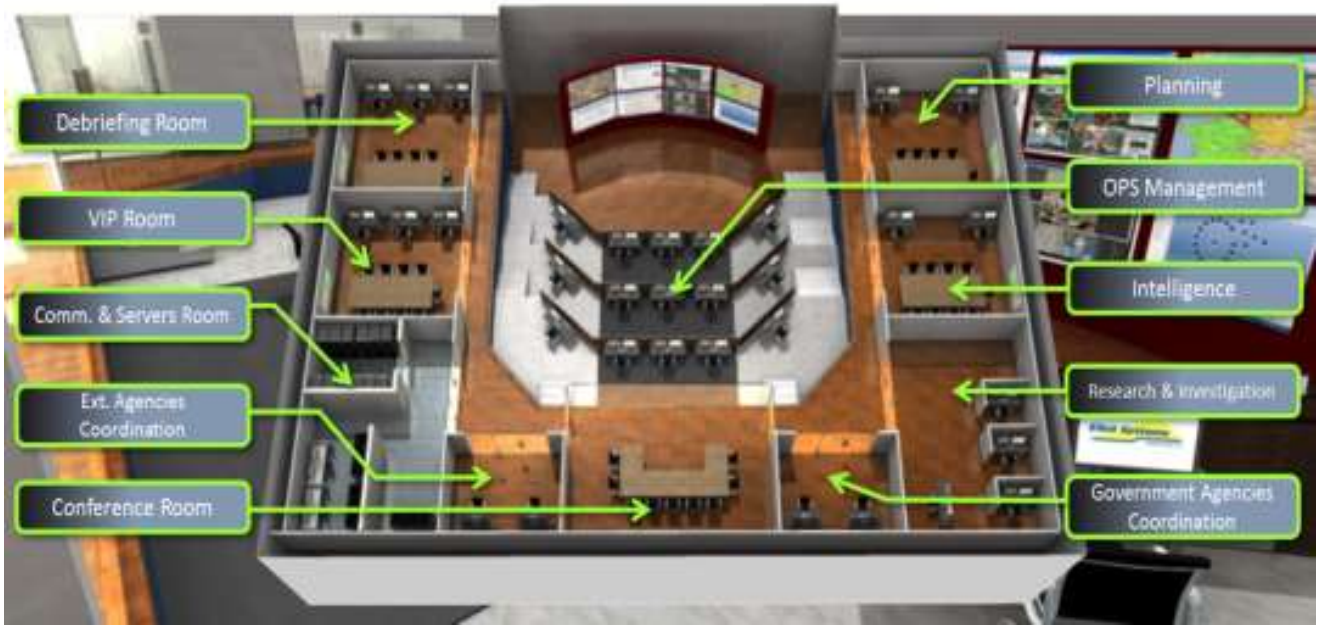
PREVENTIVE

To provide Real Time Pre event high security & Safety level

Main Concept



Intelligence C2 Center



Operation Center – principals

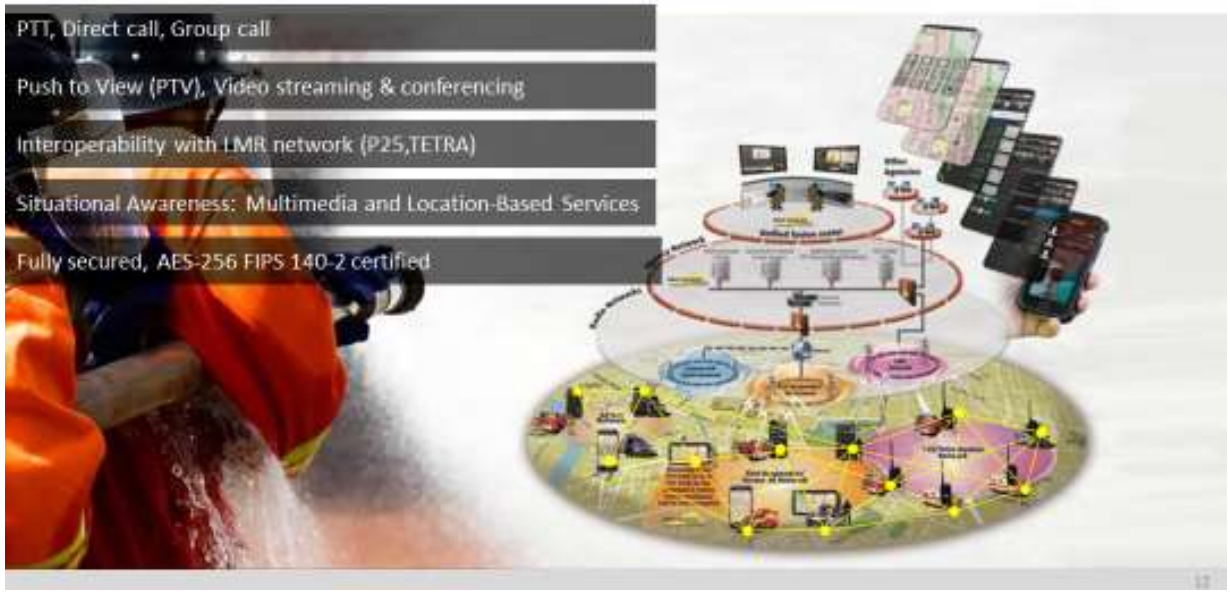
Advanced CAD System

Preparedness Management	Situation Assessment	Incident Management
Contingency Plans Support	Multi-Sensor tracking	Incident Monitoring & Analysis
Crime Prevention Procedures	Information Gathering & Analysis	Alert Management
Security Activities Planning	Activity Management & Control	Report Generation & Distribution
Prediction Tools	**Fleet and Forces Management**	
Training and Simulation		

Voice & Data Communications

Mission Critical Broadband Services for First Responders

- PTT, Direct call, Group call
- Push to View (PTV), Video streaming & conferencing
- Interoperability with LMR network (P25,TETRA)
- Situational Awareness: Multimedia and Location-Based Services
- Fully secured, AES-256 FIPS 140-2 certified

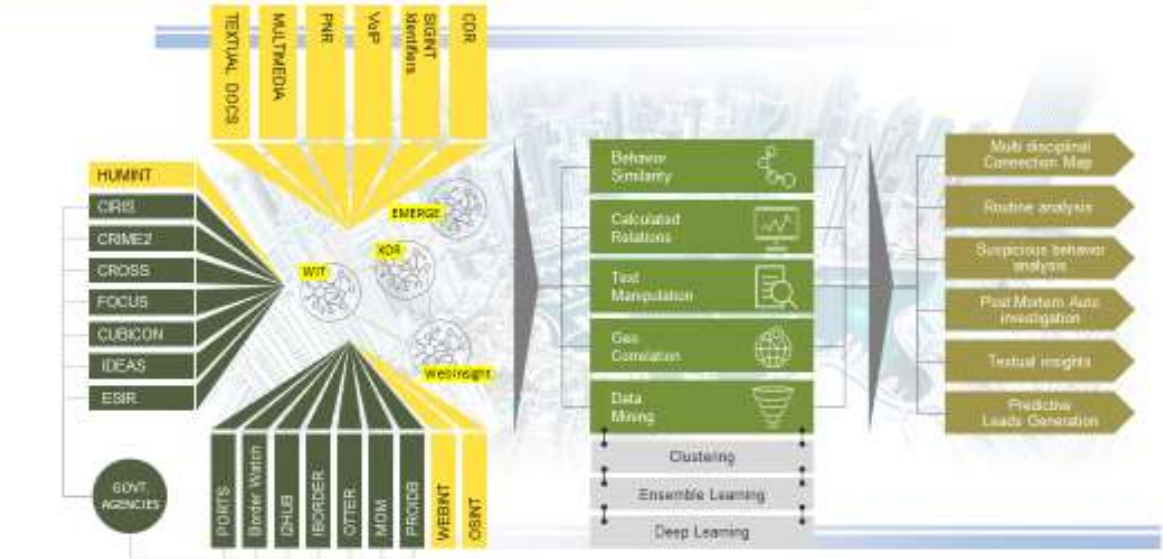


Wise Intelligence

WIT– Operational Concept

Solving Crimes Using OSInt

Security & Safety Data Fusion



3G/4G Native Cellular Platform

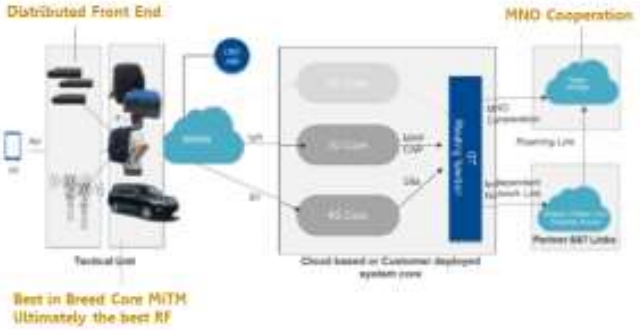
- **Single platform for multiple solutions:**
  - Intelligence (isolation, location, interception, infection)
  - Communication Control
  - Secure Mobile Private Networks
- **Most advanced technology from core to RF** – Native interception with standoff range & Mass interception
- **Proprietary capabilities for range of operational scenarios**

NICITA Native Interception Platform

Isolate & Locate
- Scan environment
- IMSI/IMEI Catcher
- Alert Engine
- Homing Device – 3G
- Denial of Service

Cyber Enabler
- Trojan Infection Platform
- **VoIP selective DOS**

Intercept & Manipulate
- Native 3G/4G **interception**
- Voice, SMS, PD
- SMS block & manipulate
- Spoof call/SMS



CYBER INTERCEPTION

Introduction

The system is a leading cyber intelligence solution that enables government, law enforcement and intelligence agencies to remotely extract valuable intelligence from any IOT or mobile device.

This unique solution was developed to provide governments, law enforcement and intelligence agencies with tools to answer the new communications interception challenges in today's highly dynamic cyber battlefield.

The system gives the ability to collect all information from IOT and mobile devices, using new interception ways which enable a substantial technology gap to deliver the most accurate and complete intelligence for any security agencies.

The Interception Challenge

The rapidly growing and dynamic of the mobile communications market bring new devices to the market, new operating systems and applications on a daily basis, which are being used by the targets who are aware of the interception technologies and systems being used by the governments and agencies.

To avoid the possibility of interception by the government or agencies, the targets change their devices and location on a daily basis; they close their phones during meetings and do not open any link, which is sent to their phones.

These changes in the target's behavior and the communications landscape, requires a new thinking of the traditional intelligence interception tools, to be able to overcome on these challenges.

What are the Challenges?

* Encryption: Use of encrypted devices and applications to convey messages.

* Abundance of communication applications: Sophisticated applications, most of which are IP-based and use proprietary protocols.

* Target outside interception: Targets' communications are often inaccessible (e.g., targets are roaming, face-to-face meetings, use of private networks, etc.)

* Use of various identities which are almost impossible to track and trace.

* Frequent replacement of SIM cards to avoid interception.

* Data extraction: The information is not sent over the network or shared with other parties and is only available on the end-user device.

* Complex and expensive implementation: As communications become increasingly complex, more network interfaces are needed. Setting up these interfaces with service providers is a lengthy and expensive process and requires regulation and standardization.

What are today solutions?

Until the above mentioned challenges are addressed and resolved, criminal and terrorist targets are likely "safe" from standard and legacy interception systems, meaning that valuable intelligence is being lost. The solutions being used today, as written below, deliver only partial intelligence, leaving the organizations with substantial intelligence gaps.

- Passive interception - Requires very deep and tight relationships with local service providers (cellular, Internet and PSTN providers). However, most contemporary communications is comprised of IP-based traffic, which is extremely difficult to monitor with passive interception due to its use of encryption and proprietary protocols.
- Tactical GSM interception solutions effectively monitor voice calls and text messages in GSM networks. When advanced cellular technologies are deployed (3G and LTE networks), these solutions become less efficient. In such cases, it is required to violently downgrade the target to a GSM-based network, which noticeably impacts the user experience and functionality.
- Malware presumably provides access to the target's mobile device. However, it is not completely transparent and requires the target's involvement to be installed on their devices. This type of engagement usually takes the form of multiple confirmations and approvals before the malware is functional. Most targets are unlikely to be fooled into cooperating with malware due to their high level of sensitivity for privacy in their communications. In addition, such malware is likely to be vulnerable to most commercially available anti-virus and anti-spyware software. As such, they leave traces and are easily detected on the device.
- Cyber intelligence, remotely and covertly intelligence from virtually any mobile device. This solution is able to penetrate popular smartphones operating systems by deploying invisible software on the target device. This agent then extracts and securely transmits the collected data for analysis. Installation is performed remotely (over-the-air), does not require any action from or engagement with the target, and leaves no traces whatsoever on the device.

Today solution systems – The problems

- Targets aware of the above technologies.
- Targets change their phones on a daily basis.
- Targets change their sim card on a daily basis.
- Targets off their phones during meetings.
- Targets change their location very often.
- Targets off their phones in their houses and offices.
- Targets do not open any link sent to their phones.
- Government/Agencies need to know the target phone number/IMEI/IMSI.

Our System and its benefits

Our system offers law enforcement agencies and governments the ability to collect intel in many different ways and from many different devices at real time with a unique command and control backend that give the agencies many advanced cyber capabilities as they never had before.
All attacks within our system are done remotely by the agencies and do not require physical distance to target in order to conduct.

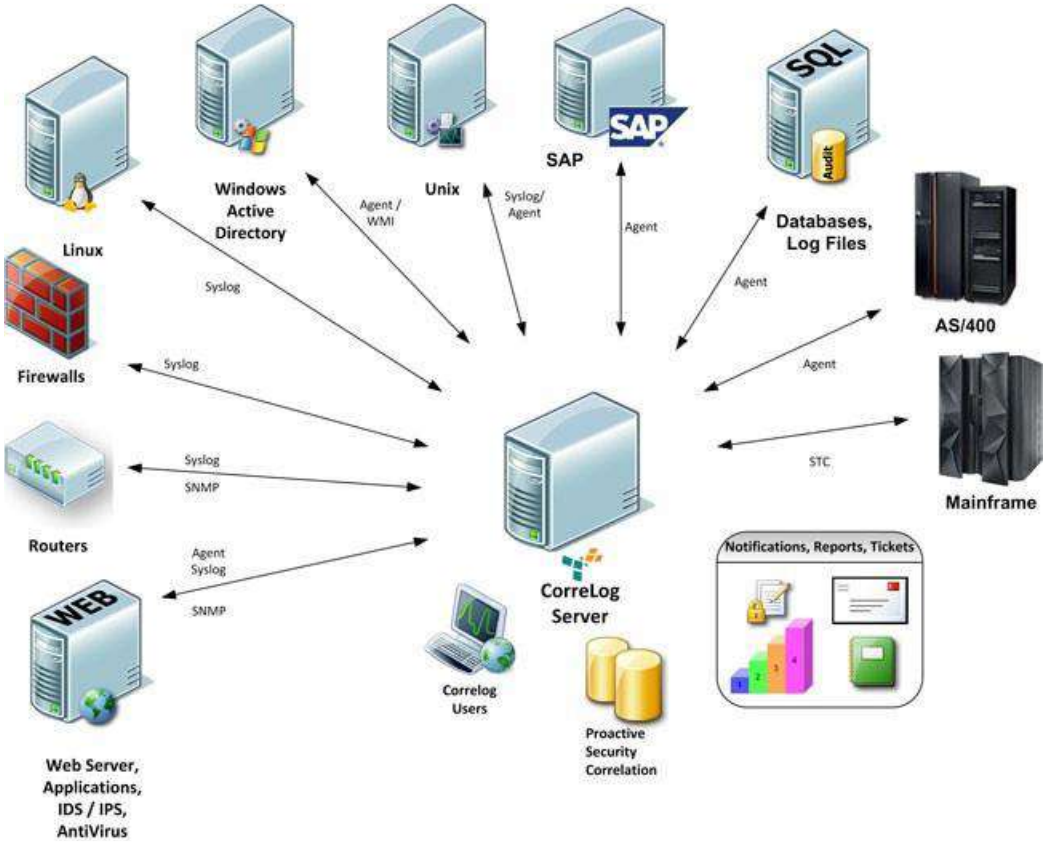
Some of our advanced features:

1. Many remote attack vectors: SMS, Email, WhatsApp, Telegram, Viber, or any other way that a link can be sent.
2. Supports many infection methods and many different devices such as: Mobile phones, Routers, Modems, DVR's, NVR's, Smart TV's, SIP phones, PBX and many more IoT devices.
3. Both recon and attack mode gives the agencies both capabilities at real time, ability to collect full recon on targets internal network remotely and ability to infect any vulnerable device within that internal network.
4. Locate-Hear-See feature: state of the art capability to locate target while activating microphone at real time to hear the surrounding while the system connects to CCTV cameras around the location of the target to also see him in real time.
5. Intercept targets traffic remotely to collect data or manipulate network activities.
6. ONE command and control center for all devices and capabilities with correlation engine.
7. Bypass any encryption method used by targets such as: WhatsApp, telegram, signal, wicker and many more, even privately developed encryption applications.

Technology Highlights

In today's cyber reality governments and law enforcement agencies use cyber capabilities and tools that are not fit or do not give the full answer for the ever-growing evolution in technology.
As written above the targets are aware of the existing systems and use any tools available in the market to avoid detection.
Our system gives a solution that does both recon and attack remotely.
Ability of interception the target without knowing his phone number/IMEI/IMSI.

Our Security Operations Centre (SOC)



What is the SOC?

Security Operations Monitoring Centre is a dedicated information security centre that monitors identifies and responds to cyber events.

SOC is the "core" of the organization, and is in fact the first body to experience a cyber event in the organization.

Its main mission is to identify and monitor real-time events, conduct a preliminary investigation (Real-Time) and deeper as well as making a quick response to the event and finally isolating it to the point of extraction and containment.

The SOC can be from one single critic or analyst who visits and monitors events to a large Centre A large number of controllers and analysts. As mentioned, its main purpose is to monitor networks, systems, devices sensitive edge and resources that can damage an organization's image, business and even damage its assets significantly.

SIEMSIEM System Information Event Manager.

In view of its importance, this system is a technological function primary and of paramount importance in monitoring Centers.

SIEM can receive logs from many systems in the organization, process information, and finally present it as a clear incident, after analysis to an analyst at SOC, or in other words, the information comes "chewed" and ripe for treatment.

How a security operations center works?

Rather than being focused on developing security strategy, designing security architecture, or implementing protective measures, the SOC team is responsible for the ongoing, operational component of enterprise information security. Security operations center staff is comprised primarily of security analysts who work together to detect, analyze, respond to, report on, and prevent cybersecurity incidents.

Additional capabilities of some SOCs can include advanced forensic analysis, cryptanalysis, and malware

reverse engineering to analyze incidents.

The first step in establishing an organization's SOC is to clearly define a strategy that incorporates

business-specific goals from various departments as well as input and support from executives. Once the strategy has been developed, the infrastructure required to support that strategy must be implemented.

Typical SOC infrastructure includes firewalls, IPS/IDS, breach detection solutions, probes, and a security information and event management (SIEM) system. Technology should be in place to collect data via data flows, telemetry, packet capture, syslog, and other methods so that data activity can be correlated and analyzed by SOC staff. The security operations center also monitors networks and endpoints for vulnerabilities in order to protect sensitive data and comply with industry or government regulations.

Benefits of having a security operations center

The key benefit of having a security operations center is the improvement of security incident detection through continuous monitoring and analysis of data activity. By analyzing this activity across an organization's networks, endpoints, servers, and databases around the clock, SOC teams are critical to ensure timely detection and response of security incidents. The 24/7 monitoring provided by a SOC gives organizations an advantage to defend against incidents and intrusions, regardless of source, time of day, or attack type. The gap between attackers' time to compromise and enterprises' time to detection is well documented in annual Data Breach Investigations Reports, and having a security operations center helps organizations close that gap and stay on top of the threats facing their environments.

Truly successful SOCs utilize security automation to become effective and efficient. By combining highly skilled security analysts with security automation, organizations increase their analytics power to enhance security measures and better defend against data breaches and cyber-attacks. Many organizations that do not have the in-house resources to accomplish this turn to managed security service providers that offer SOC services.

Here are some of the benefits of the system's broad basket that can be implemented with the help of:

1. Compliance with regulations and regulations) ISO 27000, ISO 27001, ISO27002 and

ISO 27003 (as applied by laws and reports).

2. Various cuts, dashboards and initial exploration capability.

3. Manage and maintain long-term logs.

4. Convenient management of all system functions from one central location.

5. Continuous monitoring and response to events.

6. Receive real-time alerts from various systems based on predefined logic and based on

Anomalies.

7. Saving logs as RAW Events to legal processes.

8. Compliance with regulations and standards by applying laws and reports.

9. Generating reports and views.

10. Reliability of information.

11. Verifies enforcement and policy violations.

12. Ability to cross-correlate information between different and diverse systems to create real-time organizational snapshot in real time and compared to other periods High-Tech SOC as a Service (MSS Managed Security Services).

Financial organizations, government agencies, and defense agencies collect and analyze security-relevant data from multiple huge variety of information sources, due to the sheer volume of such data, especially in large organizations, most companies the SOC uses an event management system (SIEM) to collect all data from different systems and apply rules, rules and alerts for generating alerts from this information.

The process of getting the information to SIEM

The information that comes to SIEM undergoes normalization, aggregation, filtering and flattening and enrichment processes that the incident is crude and obvious.

The process of normalization came to maintain a standard. An enterprise environment can have dozens and hundreds of types and structures various logos. Each component that reports events to the collection components does it differently.

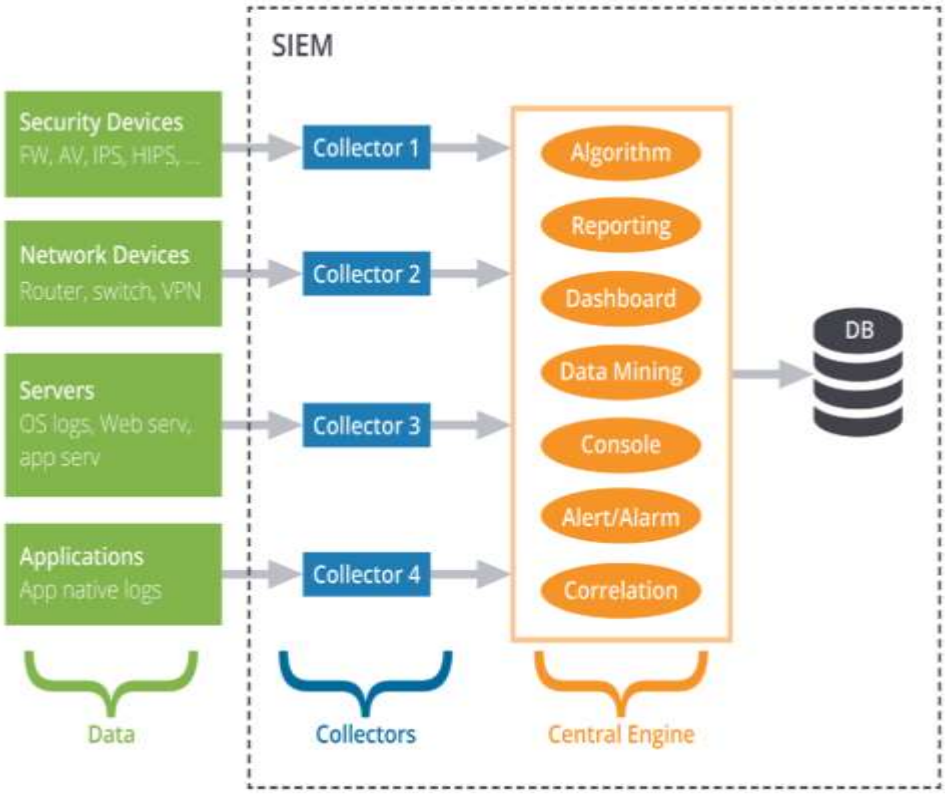
Aggregation: Network components tend to keep several log lines on identical events. Collecting all of these events can greatly strain the organization's resources, so it is possible to collect a number of pre-defined events as one single event with a field that counts the amount of events consolidated. Typically, this option is not enabled by default and should be enabled after analyzing the information obtained from the system from which the events are collected.

Filtering: Another option designed to alleviate the load that collection can create is filtering the collected events. You can define that events of particular value are unattractive and therefore do not need to be collected, for example, you can define that accept events on an internal Firewall in the organization are irrelevant and only drop events must be collected. This option makes it easier very much about the organization's resources and allows only relevant events to be focused and focused mainly on what is defined.

Filtering: The system knows how to make a catalog or / and category. These fields allow the system to determine in a way exactly what type of event was accepted into the system.

The SIEM receives the information from the collectors who collect the information from the various sources.

Basic drawing of SIEM architecture:



Sources of information:

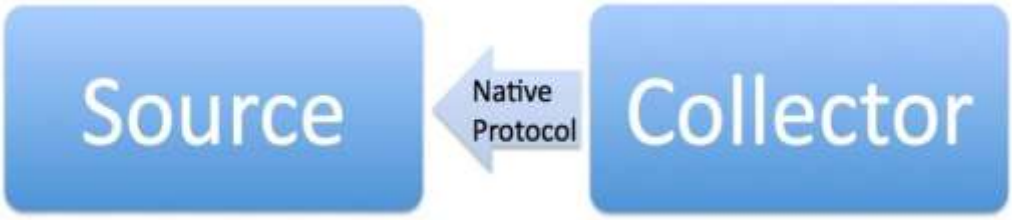
As mentioned, there are many different sources that include applications and applications, operating systems, firewalls, routers and switches, IPS / IDS systems, EPS (End Point Security) systems and virtual machines that generate data.

We can even collect network traffic directly from the network.

Collector (Collector) is an assembler whose job is to collect the events from the various devices.

The collector can come in various shapes and forms:

1. Remote code communicates directly with the device on the network:



2. An agent writes code to a dedicated log pool:

3. The collector collects a log file:

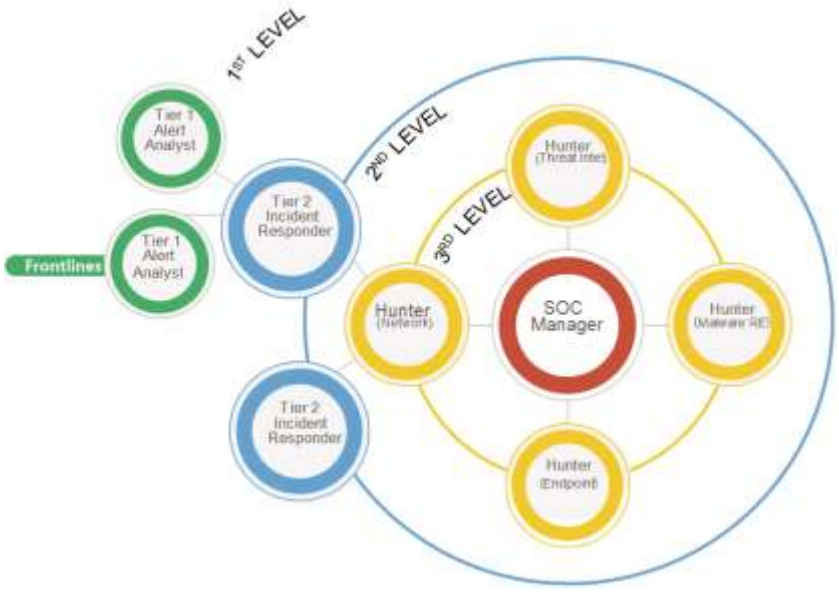
As this technology has evolved over the years, organizations are not only satisfied with the information flowing to SIEM but are also gathering more and more information from external sources such as "Cyber Intelligence Information" to get a complete snapshot and try to understand an event most accurately so that analysts can decide how to respond.

Over time, SOC centres develop the ability to consume and leverage intelligence threats from past events and information sharing sources such as intelligence providers, industry partners, law enforcement cybercrimes, and information sharing organizations (such as ISACs).

Systems "alongside the SIEM" later in the paragraph raises, as the SIEM SOC world evolves, so does its accompanying technology. Nowadays, there are quite a few products whose job is to fine-tune the raw information that comes to SIEM and to show the alert most accurately with a limited number of False Positive alerts. At the same time, these systems can guide the analyst and present an organizational holistic picture of the event's severity, a look at the SOC conceptualization of care, contact contacts, an overview of event items by timeline, mixed entities and the directionality and flow of the various operations. Another reason why organizations purchase these types of systems is because the system allows the manager to have complete control over the SOC arena by determining ways of responding and creating a structured book, thus ensuring that the event handling process is the same throughout its life cycle regardless of specific knowledge or reliance on written procedures.

Another advantage of these systems is that they can be interface to SIEM with the API, which means that any Alert or Event that comes to SIEM will reach these systems as well, without missing a log on the way.

Security Operations Centre Organizational chart:



Six steps from the time a cyber event erupts

Readiness:

SOC readiness for any scenario, from formulating and implementing appropriate security measures to ensure the continuous operation of business services, response procedures in accordance with the applicable SIEM laws, critical computer systems and infrastructure, up-to-date technology and security systems, and up to competent personnel Knowing to act, respond and thwart any event that may materialize. Establishing a methodology and managing an organized event with the understanding that targeted attacks can disable an organization in a short time and cause it business and image damage.

Identify/Monitor:

Identify/Monitor Organizational understanding development in order to manage cyber risks to systems and information assets. The actions taken at this stage are at the basic level of understanding the business context, the resources that support the critical functions and the identification of the cyber risks to which they are exposed. Taking these actions allows the organization to focus and prioritize its efforts in line with its organizational risk management strategy and business needs. This discipline concerns, among others, the following aspects: Information Asset Management, Understanding the Business Environment, Information Security Governance, and Risk Management.

Protection:

Formulation and implementation of protection systems to ensure the continuous operation of business services, servers and enterprise assets. This function relates, among other things, to the following aspects: relevant laws (SIEM), rapid response to the incident, isolation of the affected area, characterization of one new law for a period against existing threats.

Response:

Develop and implement the actions to be taken when identifying a cyber event. The response capability allows containing the effect of the cyber event after it occurs. This discipline concerns, among others, the following aspects: Planning a response to a cyber event, forensic investigation and communication with various parties, commercial investigative tools and continuous improvement by creating automatic investigation options.

Recovery and containment:

Formulate a series of actions designed to strengthen recovery and rehabilitation programs while maintaining business continuity and inclusion because of a cyber event. The recovery allows for quick return to normal operation while minimizing the negative consequences of a cyber event. This discipline concerns, among others, the following aspects: recovery planning, improvements and communication.

Practice and learning:

During or after recovery, lessons will be learned about the event that was intended to reach the next event with maximum readiness. This includes getting out of work, reducing network predators, absorbing new systems, and improving laws.

SOC Features

- **Threat detection –** At the heart of any cybersecurity system is threat detection. Business networks are subject to a wide range of potential threats, from data breaches to viruses to ransomware and more. Our team of skilled cybersecurity experts are constantly updating their knowledge and their lexicon of malware to detect any threat to a system coming from any direction and to deal with it before it can damage a company's business or its reputation.
- **Risk and liability assessment** – For hackers to get into any system and do damage, they need a vulnerability to exploit, so it needs to find out where the vulnerabilities are and to covers all the potential holes in the network so they can be plugged up before a malicious actor finds them. Whether the problem is inadequate data protection, failure to attend to third-party risks, a lack of awareness of potential threats or other vulnerability issues, they needs to be found — to be able to clear them up fast.
- **Advanced correlation** – Typical threat detection operates by using a standard set of rules to identify and score potential threat encounters. These are based on information regarding the company's valued assets to give the maximum protection against potential threats, using advanced correlation can be used to generate threat data in real-time and from the historical record.
- **24/7 network monitoring** – Cybercriminals will patiently wait until your system appears to be the most vulnerable to strike. It is necessary to protect the system 24/7, so there are no soft spots for cyber hackers to have a better chance of creating a breach.
- **Real-time alerts and rapid response** – One of the most vital elements as to how devastating a cyberattack will be is how quickly can respond to it. If there is an attempt to breach the system, every minute that is not be aware of it, is a minute that the attack is continue, it is also a time that the company could be losing megabytes of data. This is why our SOC-as-a-service comes with real-time alerts and rapid response, so once it happen, it will be alerted immediately as an intrusion attempt occurs.
- **Malicious activity remediation** – Discovering malicious activity using the SOC-as-a-service, which includes the most up-to-date antivirus and anti-malware programs.

Incident management – One of the biggest reasons companies have difficulty remediating security breaches or preventing future breaches is poor incident management. Security events need to be reported in full as soon as they happen so your network security systems can be adjusted accordingly. Using the SOC service, an access will be given to a complete incident management solution that includes incident log management, in-depth incident summaries and resolution workflows.

Our Unique Mobile Bandwidth and Memory Monitor App

The Product (The Application)

As first in the market, Mobile Bandwidth and Memory Monitor App can be used by the Government, Army, Secret Services and other official sectors.

All the above sectors are vulnerable to industrial espionage or the theft of information or any other purpose that is unlawful.

All of these sectors are concern about their privacy and will appreciate the opportunity of having the ability to protect their privacy and to block any attempt to penetrate their privacy.

Our app will monitor and log all bandwidth and memory usage used the apps installed on a mobile device.

* Log file will be detailed and be saved on servers.

* Log file is logging all apps activities online means all bandwidth (download and upload) and will be able to recognize traffic flow as far as incoming data and outgoing data and where does it goes in both ends.

* App is creating unique "Data Usage Profile" for each user by "learning" her/his activities for a certain time frame, profiles will be categorized by bandwidth usage from slim (lowest) to heavy (highest).

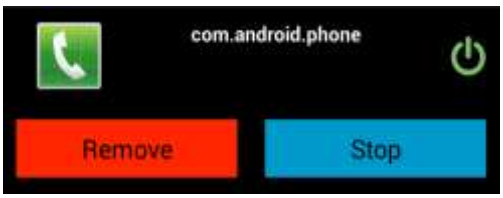
- All monitoring is being done at REAL-TIME and is logged instantly to server.

- In home page users, see the status of monitoring app.

- Real Time Bandwidth – real time monitoring of current usage of bandwidth, click on Real time bandwidth box will take users to bandwidth page.

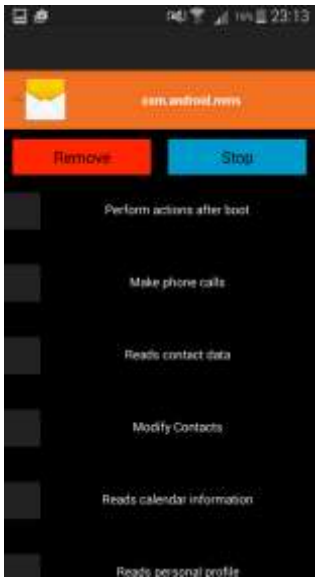
- Users will have the ability to stop or uninstall unwanted app directly from our app.

- Users will have the ability to stop or uninstall unwanted app directly from our app.



Alarms Screen

In the alarm page users see the current security issues, all issues are sorted by date and time of alert.

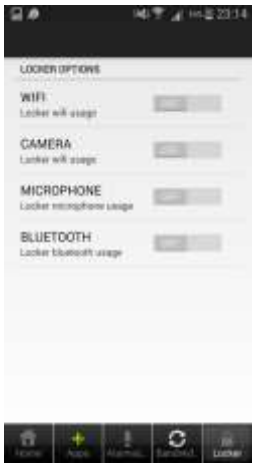


Click on alarm will take user to details and show which app triggered the alarm and what permissions this app have also will give the user the ability to stop or uninstall app.

App will run in background and will alert user even if device screen is off or device is in idle mode.

Locker Screen

In Locker screen user will have the ability to lock their Wi-Fi, Camera, microphone and Bluetooth components so they become inaccessible even to system apps.



After activating lock on component, it will not work by any means.

Trying to open the Camera no will result in error message that camera cannot be opened even that the camera is a system app.

Application Features

- App will run in background as a system service.
- Monitor Memory usage of each individual app installed on device in REAL-TIME.
- Monitor Bandwidth usage of each individual app installed on device in REAL-TIME.
- Monitor Bandwidth down to bytes usage by each individual app.
- Real-Time Bandwidth with ability to see each individual app usage at REAL-TIME.
- Monitor all apps installed on device, see which app is currently running and which do not.
- Ability to Force app to stop working.
- Monitor all apps permissions.
- Alert if any app installed on device is trying to access hardware components such as Microphone, Camera, Wi-Fi and Bluetooth even if app is a system application or operation system application.
- Alert pop up on screen at REAL-TIME and will show in notification and notifications Bar.
- Locker Option – ability to lock Microphone, Camera, Wi-Fi and Bluetooth so NO app can access them, even if it is a system or operation system app.

Why choosing us?

1. Specialize in offensive and defensive intelligence needs, using both Cyber capabilities and HUMINT, helping solve litigation issues, helped the Government in an investigation that involved leaks from the Central Bank of Nigeria, provided forensics investigation and evidence gathering.

2. Penetration testing and security audits specialize in mobile carriers and mobile devices, provides forensics investigation for mobile devices and computers, checking for eavesdropping devices.

3. “Virtual” body guards for HNWI (High net worth individuals), Celebrities, Ex govt. officials and many more, providing encrypted channels for secret and safe communications, setting up private VPN infrastructure with many different location for totally private, safe and secure browsing online.

4. Designing and building tailor-maid security products for specific usages. For example special Wi-Fi Router to identify unauthorized devices in secured environment.

5. Hardening mobile devices for more private, safe and secure usage.

6. Designing and building SOC centers for governments and enterprises, providing SOC as service solutions, a security operations center (SOC) is a facility that houses an information security team responsible for monitoring and analyzing an organization’s security posture on an ongoing basis. The SOC team’s goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work close with organizational incident response teams to ensure security issues are addressed quickly upon discovery. Security operations centers monitor and analyze activity on networks, servers, endpoints, mobile device, IoT devices, databases, applications, websites, and other systems, looking for anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.