CYBERSEAL

www.cyber-seal.net

YTTRIUM

IMSI CATCHER

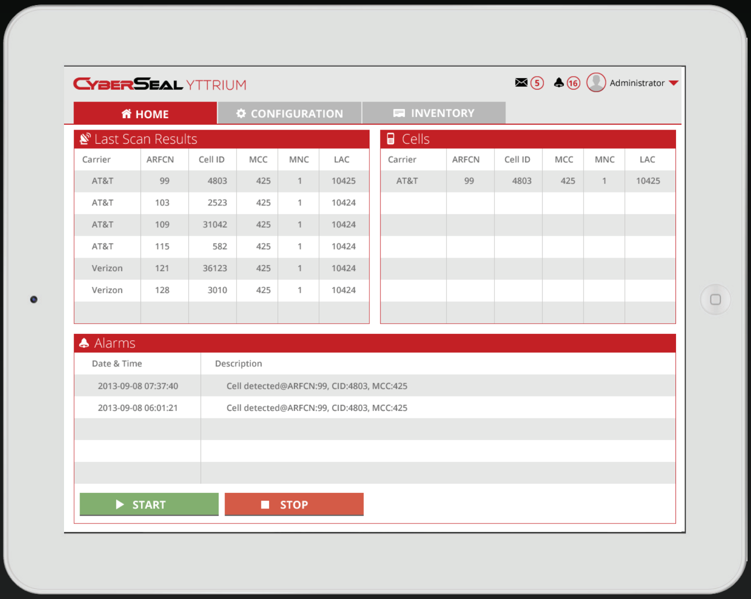
THE NEW STANDARD IN PREVENTING ILLEGAL CELL PHONE ACTIVITY IN CORRECTIONAL FACILITIES

- *Identity extraction and isolation*
- *Central Management*
- *Customizable Policies*
- *Accurate Positioning*
- *The ideal solution for controlling cell phone usage in correctional facilities*

GENERAL

The illegal use of contraband cell phones by inmatesof correctional facilities poses an increasing threat to public safety.

We are proud to present the new industry standard: Yttrium, Cyber Seal's IMSI Catcher. Yttrium was specifically designed for correctional facilities. It provides cost-effective, fixed or tactical solutions to covertly identify, locate and render useless all illegal GSM, 2G and 3G cell phones within its effective range. The system simulates a true GSM base station, forcibly reroutingall mobile communicationsthrough a central hub. This core element acquires the identities of all cell phones within its effective range and then blocks their transmissions tocellular telecomtowers.



Last Scan Results

Carrier	ARFCN	Cell ID	MCC	MNC	LAC
AT&T	99	4803	425	1	10425
AT&T	103	2523	425	1	10424
AT&T	109	31042	425	1	10424
AT&T	115	582	425	1	10424
Verizon	121	36123	425	1	10424
Verizon	128	3010	425	1	10424

Cells

Carrier	ARFCN	Cell ID	MCC	MNC	LAC
AT&T	99	4803	425	1	10425

Alarms

Date & Time	Description
2013-09-08 07:37:40	Cell detected@ARFCN:99, CID:4803, MCC:425
2013-09-08 06:01:21	Cell detected@ARFCN:99, CID:4803, MCC:425

FEATURES

IDENTITY EXTRACTION

Yttrium extracts all mobile identities from GSM cell phones (IMSI, TMSI, IMEI & IMEI SV and MSISDN, when available) and notifies the system administrator of any activity performed by a cell phone. Employing the concept of 'blacklist vs. whitelist', illegal cell phones are identified and isolated while preserving the right of law-abiding citizens to enjoy the benefits of mobile services without disruption.

CUSTOMIZABLE POLICIES

Yttrium enables the administrator to enforce a variety ofpolicies toward contrabandcellphones. It addresses specific operational requirements and diverse regulatory demands by using one the following methods:

- *White-listing and black-listing*
- *Disabling of illegal devicesuntil power reset (i.e. battery removal)*
- *Blocking of calls, SMSs or data usage*
- *Permittinga fixed number of calls withina predefined timeframe*
- *Sending SMSs to illegal phones notifying them that they are blocked*
- *Allowing emergency (911) calls.*

CENTRAL MANAGEMENT

Yttrium consists of a command centerand peripheral units. Central management is located in the command and control room, while the peripheral units provide flexibility in covering any required area. The system can be configured for fully automated or manual operation.

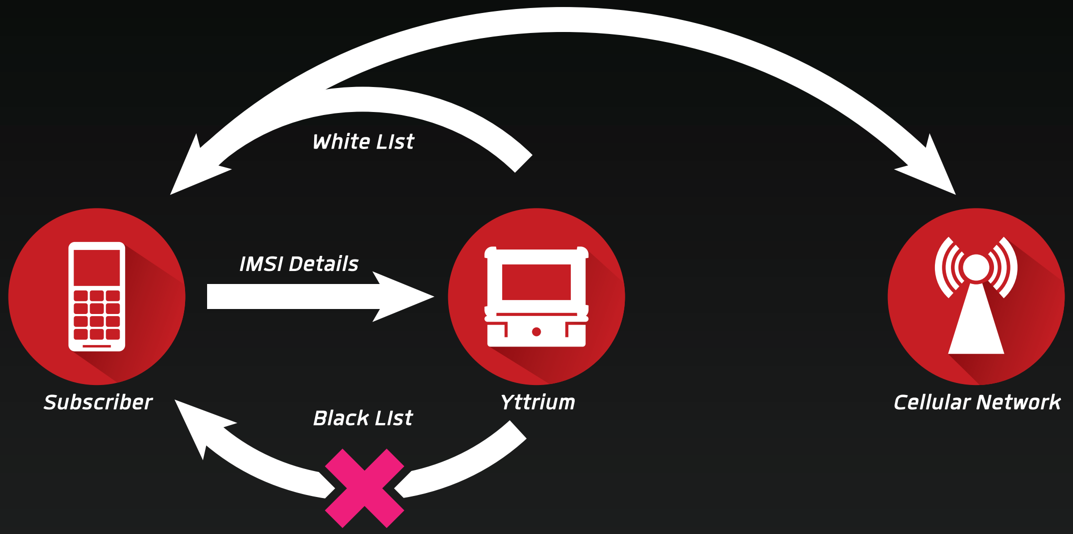
The system is equipped with a user-friendly interface that displays acquired phones and their identities, logs all communication attempts and provides real time alerts at switch on or switch off of blacklisted mobile devices. It also offers the capability of implementing CALEA compliant interfacing for law enforcement agencies.

Yttriumuniquely caters for fully automated cell cloning by automatically locking ontoeach phone's distinctive signature.

ACCURATE POSITIONING

The Yttrium operator can put out a silent call to a target's cell phone, forcing the phone to transmit continually without the user's knowledge,while simultaneously permitting accurate navigation to the inmate's location using a covert hand-held homing device. Other optional facilities include 'RF Fingerprinting' and standard triangulation.

CyberSeal
www.cyber-seal.net



INSTALLATION OF PERIPHERAL UNITS

Peripheral units are used to collect cellphone identities and execute predetermined policies on target phones. Units are controlled through a secure communication channel. Yttrium's peripheral units support both fixed and mobile installation, indoors or outdoors, with a coverage area of up to 1sq.km. Each can be adjusted according to on-site demands.

Peripheral units are camouflaged and tailored to the customer's specific needs. In addition, ironclad security is used to detect, prevent and alert to any tampering attempts by inmates.

Finally, Cyber Seal also provides consulting services in order to optimize peripheral unit installation and ensure full area coverage with the minimum number of units.

OPERATIONAL GUIDELINES

Yttrium's simulated GSM base station permits calls by known users (i.e., prison-authorized cell phone numbers) by handing them over to the network, but prevents others (i.e. illegal, contraband cellphones) by denying them access to the telecom network.

To allow optimal acquisition of cellphones within the system's coverage area, the following steps should be completed:

- *Selection of Effective Locations for Peripheral Units: Proper installation of peripheral units in strategic areas is imperative for optimal system operation. This requires one or several base stations configured to reach the boundaries of the compound. Prior planning will guarantee optimal usage of the hardware, while the coverage area can be controlled by modifying power output and selecting proper antennas. Distributed Antenna Systems (DAS) may be deployed for greater coverage and a more cost effective solution.*
- *Selection of Optimal Network Parameters: Proper selection of network parameters facilitates maximal acquisition. The simulated GSM base station intercepts transmissions, resulting in dependable acquisition of cellphone identities. A unique automatic algorithm ensures optimal coverage and negligible interference to existing telecom networks without prior coordination.*
- *Cellphone Acquisition: After selection of network parameters, the simulated GSM base station is ready to acquire cellphone identities. The system administrator can then create white lists and black lists and set separate policies for each group or phone. This process can be repeated every few hours to make sure all phones in range will be acquired, including phones that were switched off during the previous round.*
- *Accurate Positioning: Yttrium can locate target phone's accurately by initiating a silent call that forces the cellphone to transmit continually without its owner being notified. A covert hand held homing device then locates the transmitting device. Even if inmates have taken great care to hide their device, Yttrium can force the target's cellphone to ring, thus exposing its location.*

TECHNICAL SPECIFICATIONS & FEATURES

FEATURE	DESCRIPTION
POWER SUPPLY	
DC feed	12V w/Battery.
AC feed	110-220V
Power Consumption	Up to 50W
ENVIRONMENTAL INFO	
Operating temperature	-20°C to +50°C
Storage temperature	-40°C to +85°C
Relative humidity	0 to 90% non-condensing.
Dimensions	5200 x 400 x 188 mm.
Weight	12Kg
REGULATION	
Standards	FCC, EMC, Safety
RF	
Antenna	Directional / Omni-directional
Transmission Output Power	Up to 50dBm (100W)
Supported Frequency Bands	GSM-850 (824.0–849.0 / 869.0–894.0), P-GSM-900 (890.2–914.8 / 935.2–959.8), DCS-1800 (1710.2–1784.8 / 1805.2–1879.8), PCS-1900 (1850.0–1910.0 /1930.0–1990.0). EGSM. UMTS I 2100 (1920–1980 / 2110–2170), UMTS II 1900 (1850–1910 / 1930–1990), UMTS IV 1700 (1710–1755 / 2110–2155), UMTS V 850 (824–849 / 869–894), UMTS VII 900 (880–915 / 925–960).
INTERFACES	
Ethernet	1xGbE
USB	2xUSB 2.0
GPS	1xGPS receiver
LCD	Color, 10”, 1024*768 pixels.
Input Devices	Keyboard, Mouse
MONITOR AND CONTROL	
Central Management	Client/Server Architecture, HTTPS based, capable of managing up to 100’s of device

CyberSeal Ltd.
25 Habarzel Street, Tel-Aviv, Israel 6971035
T: (972)-3-6449991, F: (972)-3-6449992
www.cyber-seal.net

Distributed by:

Version: 1.00