Network Guard

Rogue Cellular Base Station Detection

Network Guard provides world-class situational awareness of cellular communication surveillance, interception, and attacks.

Network Guard offers a robust capability to detect and combat cellular network monitoring and interception. Network Guard's real-time data correlation and analytics engine rapidly identifies and alerts on cellular RF attacks on GSM, WCDMA, CDMA-2000 and LTE networks. Network Guard is able to detect attacks from simple DIY-built IMSI Catchers to the most sophisticated nation-state developed interception systems.

Who Needs Network Guard

Mobile device surveillance systems are being leveraged by nation states, criminal organizations and industry competitors. These groups are targeting and exploiting intelligence, stealing proprietary information and intercepting sensitive communications.

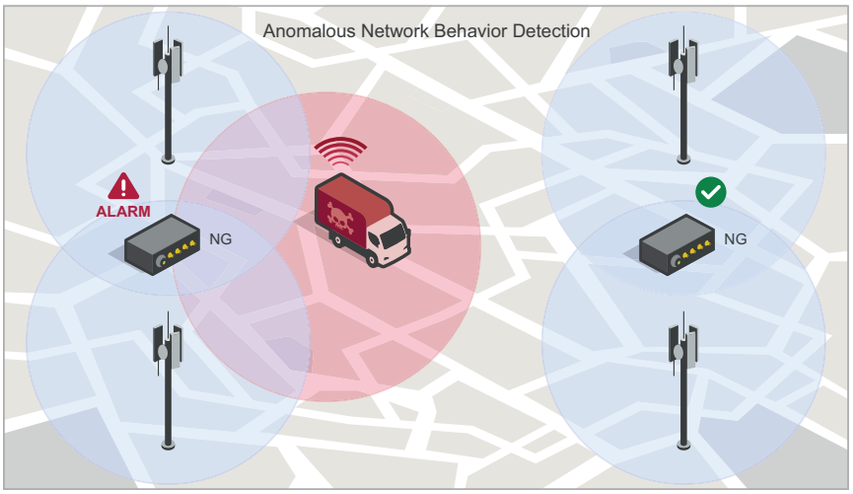
Vulnerable targets include:

- Government facilities, embassies and military bases
- Corporate enterprises, financial institutions and law firms
- Sensitive field and law enforcement operations
- Critical infrastructure

How It Works

Network Guard continually surveys all available cellular networks and performs real-time analysis on the collected data. Anomalous network behavior is detected by in-depth inspection of broadcast information from base stations. This level of inspection allows the system to immediately alert when active cellular surveillance systems are in-use. The collected data is also stored for further post-mission analytics. Post-mission analysis is rapid, detailed and can be combined with surveys from previous missions to highlight changes in the mobile networks over time.

The network survey process utilized by Network Guard is designed to detect many different exploitation techniques and signatures used by the various types of devices used for cellular network surveillance.



What It Detects

- All types of cellular network surveillance (Active, Semi-Active and Infrastructure) and hacking where bad actors can manipulate numerous variables to exploit mobile communications.
- How cellular network surveillance equipment attempts to exploit the official mobile networks.

CHARON TECHNOLOGIES

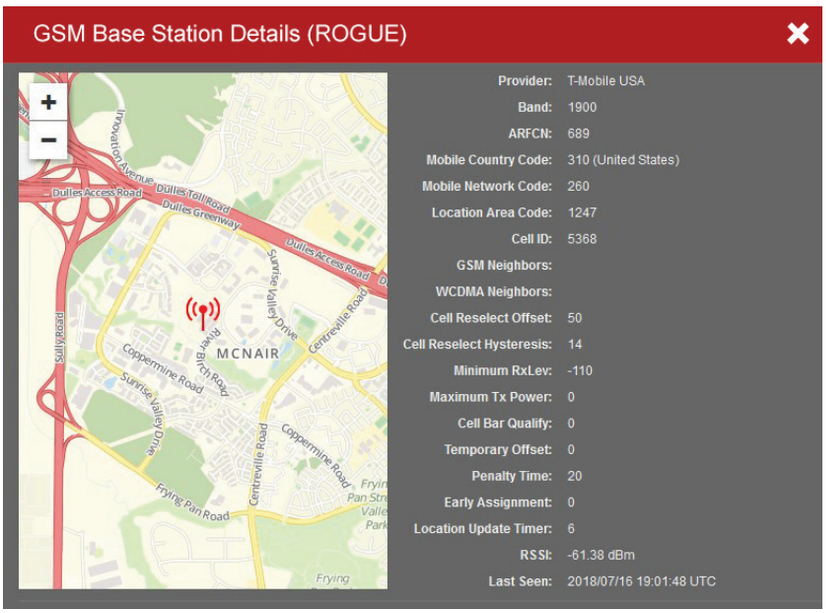
Network Guard Configurations

Tailored for various customers & scenarios:

- **Network Guard Scout** - Utilized in both static and mobile scenarios. Fully self-contained systems controlled and monitored via Ethernet or wireless devices.
- **Network Guard Connected** - Static in-place endpoints that are monitored locally or distributed units remotely monitored at a network/security operation center.

World-class Technology

- Simultaneous scanning of multiple radio access technologies
- Real-time analysis and alerting engine
- Integrated with CTL-SystemWare's Resource Manager 2 software offering direct monitoring, configuration and tasking as a single endpoint solution or part of a larger multi-sensor deployment.
- Integrated GPS for accurate positional info
- Passive cellular downlink scanning and decoding
- Web-based command and control
- Command and control over Ethernet or Wi-Fi
- Remote out-of-band communication over cellular modem
- Integrated vector mapping
- Multiple export data formats
- System can operated in autonomous mode
- Extensible platform to support future mission requirements
- Deployed with government organizations worldwide
- Designed and manufactured in the U.S.A.



Threat Characterization

The techniques behind the world's more sophisticated mobile network interception and hacking equipment have been identified over years of research and field experience. Network Guard is able to detect and alarm on all of these techniques. This includes time-based attacks and the detection and directional finding of fake base stations (cells). Network Guard is simply unmatched in technology and provides the ultimate in mobile network counter surveillance.

Networks Covered

- *GSM*
- *CDMA2000*
- *WCDMA*
- *LTE (FDD)*

"The number of sensitive communications that are taking place every day using our cell phones are increasing at an exponential rate. Regrettably most are unaware of the enormous interception and surveillance vulnerabilities that mobile communications present. Network Guard is the only product that can not only detect all forms of mobile interception and can also directionally locate the source."

Rob Mozeleski
President, Charon Technologies

Contact Us

For information or to schedule a demo, contact us at:

Charon Technologies, LLC
(703) 662-6021
info@charontech.com

CHARON TECHNOLOGIES