LOCH TECHNOLOGIES

5G & CBRS Risks and Threats

Protect your business from 5G & CBRS cyber threats.

Learn how to mitigate 5G and CBRS risks.

www.loch.io

Cellular 5G & CBRS Risks and Threats

LOCH

Navigating the Security Landscape of Cellular Networks

In the era of rapid technological advancement, cellular networks such as LTE (Long-Term Evolution) and 5G have become pivotal in delivering high-speed data and voice services. These networks of modern communication technology offer unprecedented connectivity and data transmission capabilities. However, with great advancement comes increased vulnerability. Despite their sophistication, cellular networks are not impervious to security threats and malicious attacks.

The following delves into some prevalent types of attacks targeting LTE and 5G networks. From IMSI Catcher (Stingray) attacks, which deceive mobile devices into connecting with false cell towers, to sophisticated Man-in-the-Middle (MITM) attacks manipulating communication channels, the range of threats is diverse and complex.

Denial of Service (DoS) attacks aim to overload systems, while Downgrade Attacks exploit security gaps between network generations. Moreover, the exploitation of protocol vulnerabilities, SS7 and Diameter Protocol attacks, and the creation of Fake Base Stations reveal deeper layers of potential breaches.

5G & CBRS Threat

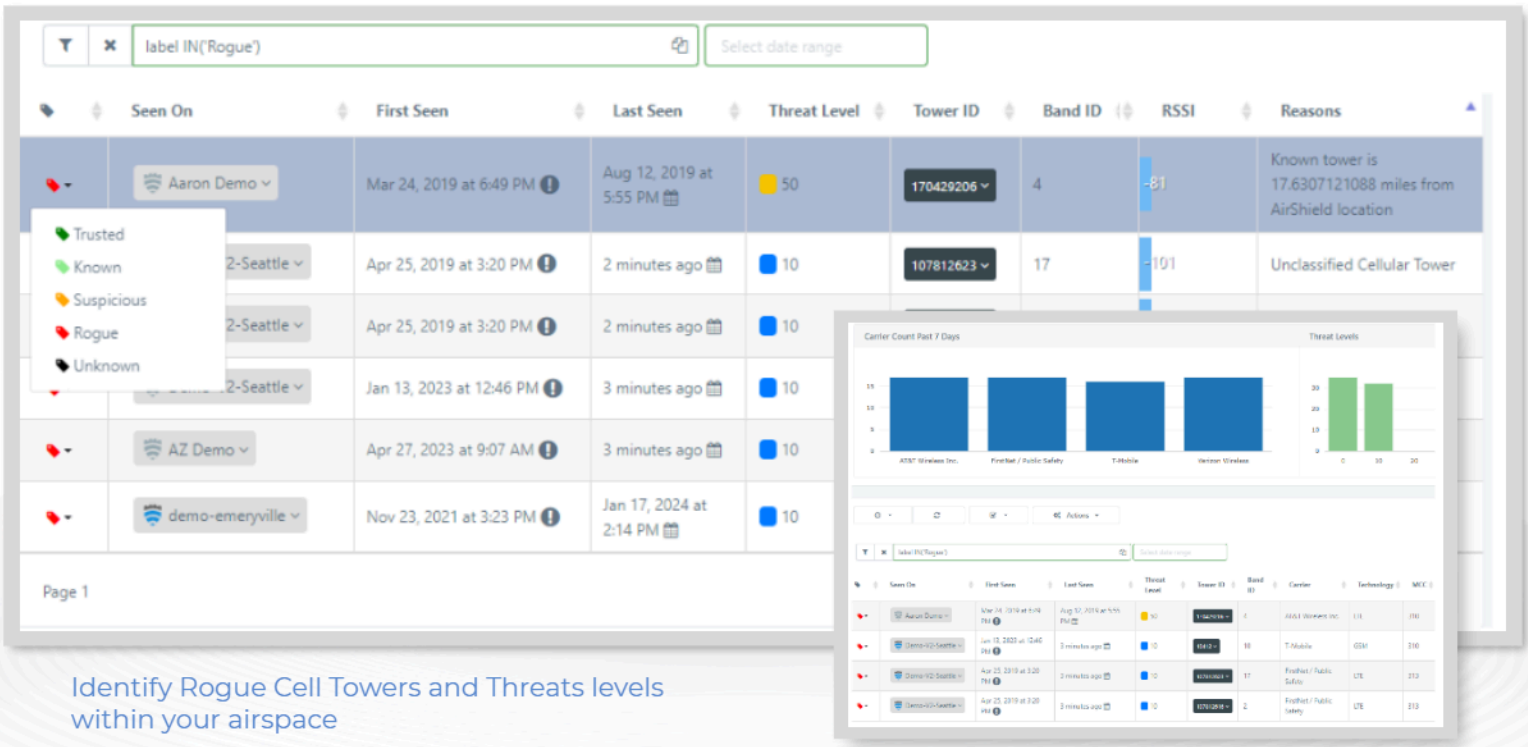
- **IMSI Catcher (Stingray) Attacks:** Devices known as IMSI catchers or "Stingrays" can masquerade as legitimate cell towers, tricking phones into connecting to them. This allows attackers to intercept calls, texts, and data, as well as track the location of mobile devices.
- **Man-in-the-Middle (MITM) Attacks:** Attackers can intercept and alter the communication between a mobile device and the network. This can be done by creating a rogue base station or exploiting vulnerabilities in the signaling protocols.
- **Denial of Service (DoS) Attacks:** These attacks can target individual users or entire networks, overloading them with traffic to degrade or disrupt service. In LTE and 5G networks, this could involve overwhelming the network's signaling channels.
- **Downgrade Attacks:** An attacker might force a device to downgrade from a more secure network (like 5G) to a less secure one (like 3G), exploiting weaker encryption and security protocols.
- **Protocol Exploits:** Vulnerabilities in the protocols used by LTE and 5G networks can be exploited to conduct various attacks, including location tracking, eavesdropping, or interrupting network services.
- **SS7 and Diameter Protocol Attacks:** These attacks exploit vulnerabilities in the Signaling System No. 7 (SS7) and Diameter protocols used for communication between different networks, enabling attackers to intercept calls and messages.
- **Fake Base Station Attacks:** Also known as "Evil Twin" attacks, these involve setting up a rogue base station to mimic a legitimate cell tower, allowing attackers to manipulate calls, messages, and data traffic. Exploiting vulnerabilities in the network can allow attackers to access and manipulate user data, leading to privacy breaches and data theft.
- **Resource Exhaustion Attacks:** By sending numerous connection requests or other signals to the network, attackers can exhaust resources, leading to service degradation or denial of service.
- **Location Tracking and Surveillance:** Exploiting weaknesses in paging protocols and other mechanisms, attackers can track the location of users without their consent.
- **Encryption Key Theft:** By exploiting vulnerabilities, attackers may be able to steal encryption keys, allowing them to decrypt and access private communications.

Cellular 5G & CBRS Risks and Threats

The risks and threats associated with Citizens Broadband Radio Service (CBRS) are not entirely the same as those for 5G, although some overlap exists; CBRS operates in the 3.5 Ghz - 3.7 GHz band and is designed for shared wireless access (similar to Wi-Fi, however, CBRS introduces unique challenges and vulnerabilities.

Specfic Threats CBRS

- **Interference:** Like 5G, CBRS faces the risk of signal interference, which can degrade service quality.
- **Unauthorized Access:** There's a risk of unauthorized access to the network, which could lead to data breaches or other security incidents.
- **Eavesdropping:** The potential for intercepting communications exists in both CBRS and 5G networks.
- **Spectrum Sharing Complexity:** CBRS uses a dynamic spectrum-sharing approach called (SAS) involving three tiers of users (Incumbent, Priority Access, and General Authorized Access). Priority Access License.
- **(PAL) Security:** Those with PAL have more control over their portion of the spectrum. However, ensuring these licensees do not face interference from General Authorized Access, is a challenge.
- **Device Authentication and Management:** In CBRS, ensuring that devices are correctly authenticated and managed within the spectrum is critical. There's a risk that unauthorized or non-compliant devices could access the spectrum.
- **Incumbent Protection:** Ensuring incumbent users (like the military) are protected from interference by commercial users is a unique aspect of CBRS—this 24/7 robust monitoring and enforcement mechanisms.
- **Spectrum Access System (SAS):** CBRS relies on a Spectrum Access System to dynamically allocate spectrum. Any compromise or malfunction in SAS could lead to widespread service disruption or security breaches.



Identify Rogue Cell Towers and Threats levels within your airspace

AirShield Wireless Airspace Defense for CBRS

AirShield lets organizations see every RF "intentional" or "unintentional" emitting device within their environment, on or off their production network, whether connecting via Cellular, Broad-Spectrum IoT, Bluetooth, or Wi-Fi.

AirShield provides comprehensive visibility into the IT, IoT, and OT (Operational Technology) threat landscape to detect, assess, and prevent risk from unmanaged, unsecured, and misconfigured IoT devices.

Wireless Attack Surface

IoT has created the world's largest attack surface, the scope of which is only broadening with the promise of 5G. Today's networks and organizations were never built to handle the volume, velocity, and hyper-connectivity of smart devices in the business environment.

With 80% of devices now wirelessly connected, wireless has quickly become the new network and new attack surface - the invisible threat. Yet, most organizations (both business and government) still struggle to identify wireless devices within their environment — creating new security blind spots.

Zero Trust for Cellular, Broad-Spectrum IoT, Bluetooth/BLE, and Wi-Fi. Wireless Security

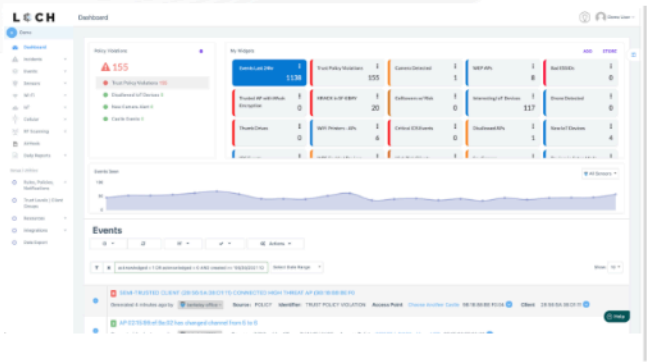
- Visibility - Discover all cellular wireless devices within your environment.
- Protection - Automatically identify unmanaged, unsecured, and misconfigured IoT and OT devices.
- Non-Intrusive - Passive monitoring of airwaves for enforcement of zero-trust policies.
- Easy to Deploy - No Ethernet required. Integrated cellular back-haul for real-tim access to cloud wireless threat analytics.

Passive monitoring of the Cellular airwaves for next generation Wireless Airspace Defense — eliminating the RF espionage threat to the enterprise.

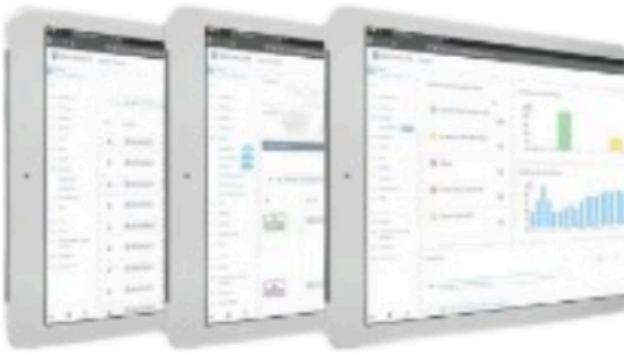
AirShield Wireless Airspace Defense

Key Features

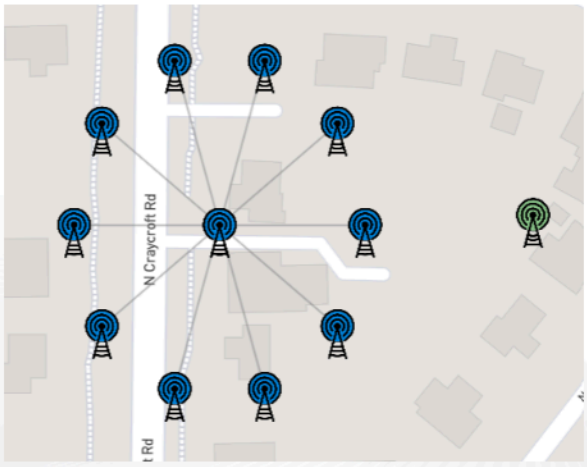
- Enabled - AirShield sensors connect to the cloud or on-premise server for asset discovery, classification, and incident response.
- Real-time Data Analytics -Identify unacceptable wireless vulnerabilities in managed and unmanaged devices.
- Customizable Software Defined Radio - monitors the new Wi-Fi 6/6E and CBRS / 5G spectrum (300Mhz to 6Ghz) to detect new and wireless threats
- Critical Path to Exposure("") Reporting- Raise awareness of the growing wireless security risks.
- Threat Hunting - AirShield offers a threat-hunting application to find "the needle in the haystack." - locate nefarious wireless devices quickly.
- AirShield sensor covers 25,000 sq ft and is at an affordable cost, which includes cloud access.
- AirShield uses AI and ML for asset discovery, asset classification, and behavior analysis, which provides better fidelity and fewer false positives).
- AI/ML Auto Encoders, Zcode with Ngram for wireless deep packet inspection.
- AirShield offers offensive pen-testing capabilities, i.e., password validation and cracking.
- IoT Rogue - Rogue communication and data exfiltration.
- SIM Port Hijack - Loss of control over your SIM connectivity.
- Extensive wireless attack library detection capabilities.
- Rogue Cell Tower - Detect Stingrays and SIM devices are connecting to an evil twin cell tower.
- Cellular UE/device spectrum monitoring.



Centralized Management of Cellular, IoT, BT & Wi-Fi



Audit and Compliance Reporting



Validate CBRS connections