

Invisible Threats. Visible Protection.

BENEFITS OF USING AN SDR (SOFTWARE- DEFINED RADIO) FOR WIRELESS CYBERSECURITY



Integrating SDRs into your security strategy can significantly enhance your ability to detect and prevent sophisticated, "unseen" cyber threats within your wireless environment.

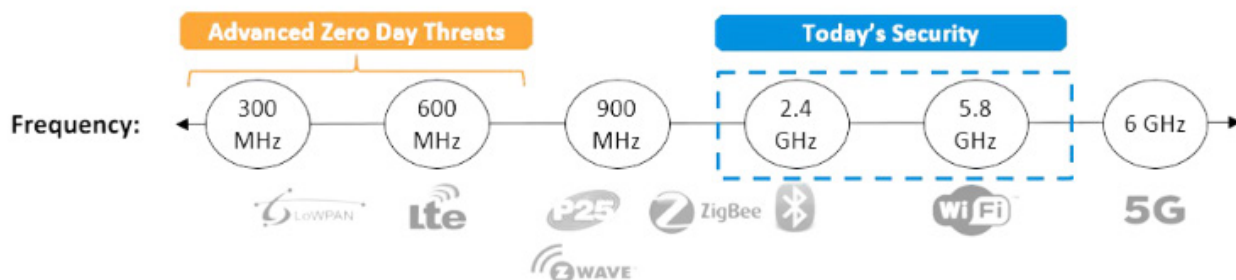
Benefits of Using an SDR (Software Defined Radio) for Wireless Cybersecurity

In today's rapidly evolving digital threat landscape, the integration of software-defined radio (SDR) into wireless security strategies represents a pivotal advancement in safeguarding against sophisticated cyber threats. SDR technology stands at the forefront of addressing the unique challenges presented by the expanding realm of the Internet of Things (IoT) and wireless communications. By harnessing the versatility and comprehensive spectrum coverage of SDR, organizations can dynamically adapt to detection new threats, ensuring proactive and resilient defense mechanisms. This technological innovation enables real-time threat detection, broad-spectrum monitoring, and a high degree of flexibility in responding to and mitigating risks. The adaptability of SDR to evolving threats, coupled with its capability for deep integration into existing cybersecurity infrastructures, makes it an indispensable tool in maintaining the integrity and security of wireless networks. As we navigate the complexities of this increasingly wireless world, the SDR role in enhancing security measures is crucial and a game-changer in the proactive defense against emerging and sophisticated cyber threats.



Integrating SDRs into your security strategy can significantly enhance your ability to detect and prevent sophisticated cyber threats across the multi-frequency wireless domain. By leveraging AirShields Software Defined Radio (SDR) capabilities, it offers a comprehensive frequency detection range, flexibility and spectrum coverage, and dynamic adaptability, which aligns with the need for advanced and proactive security measures in the increasingly wireless world of IoT.

Frequency Detection Range





With the growing reliance on wireless technologies in IoT devices, addressing the invisible threat in this new attack surface becomes paramount. Software Defined Radios (SDRs) play a crucial role in enhancing wireless security and preventing high-profile cyber attacks in several ways:



Broad Spectrum Monitoring:

SDRs can monitor various frequencies, including cellular, CBRS (Citizens Broadband Radio Service), IoT-specific spectrums, Bluetooth, and GPS signals. This allows for the early detection of unauthorized or suspicious activities across these frequencies.



Real-Time Threat Detection:

SDRs can be programmed to identify specific patterns or anomalies in wireless signals that may indicate a cyber attack, such as unusual signal strengths, spoofed communication, or unauthorized access attempts.



Dynamic Response Capabilities:

Given their programmable nature, SDRs can be quickly reconfigured to respond to emerging threats or to adapt to changes in the wireless technology landscape, ensuring continual protection against new vulnerabilities.



Identification of EMI (Electromagnetic Interference):

SDRs can detect and analyze sources of EMI, which may indicate Malicious activities stemming from compromised hardware, counterfeit products/microchips on the motherboard, creating stealthy covert communications.



GPS Spoofing and Jamming Detection:

By monitoring GPS frequencies, SDRs can detect spoofing and jamming attempts, ensuring the integrity and reliability of location data, which is crucial for many IoT applications.



Integration with Security Systems:

SDRs can be integrated with existing SIEM/SOAR cybersecurity systems and NDR infrastructure, enhancing the ability to detect and respond to wireless threats in real-time.



Training and Simulation:

SDRs can be used for cybersecurity training, simulating various attack scenarios to test and improve wireless network defenses.



Developing Countermeasures:

Once a threat is detected, SDRs can assist in developing countermeasures, such as signal jamming, encryption enhancements, or protocol changes to mitigate the risk.



Compliance and Regulation Adherence:

Ensuring wireless communications comply with regulatory standards and detecting deviations that might indicate security breaches.



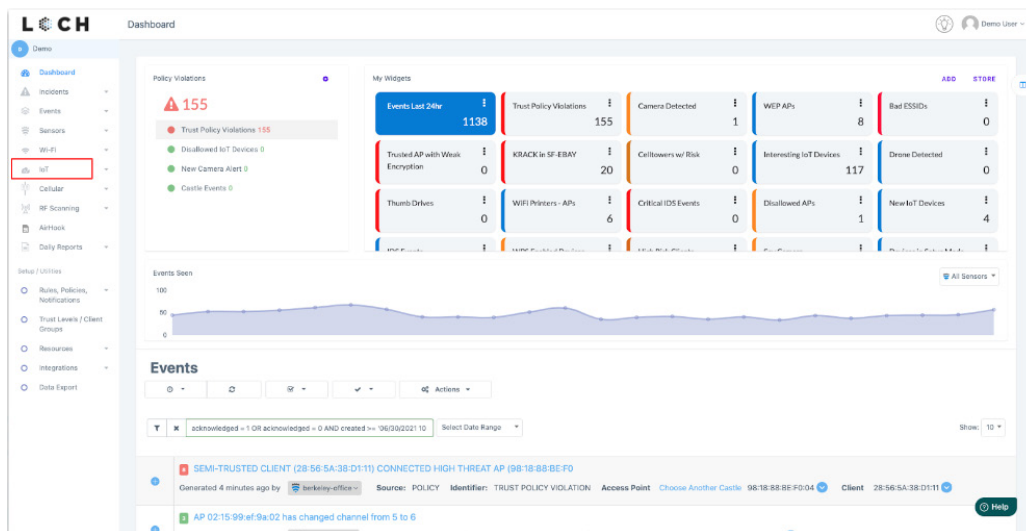
Forensic Analysis:

After an attack, SDRs can aid in forensic analysis by providing insights into how the attack was carried out, helping to strengthen defenses against future attacks.



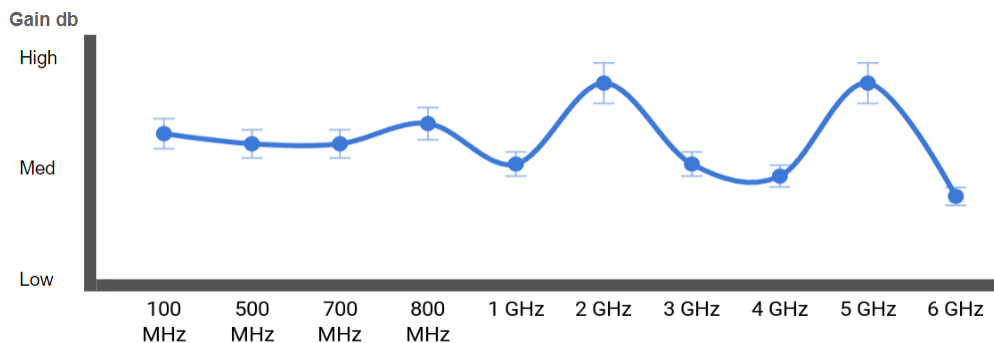
Wireless Airspace Defense - a new era in cybersecurity

LOCH's AirShield Software-Defined Radio offers an advanced solution for real-time analysis and threat detection across various wireless deployments, including cellular, CBRS, broad-spectrum IoT, Bluetooth, GPS, EMI, and WiFi. The AirShield Wireless Airspace Defense system delivers a significant competitive edge over fixed chipset WLAN solutions. The platform is dynamically aligned with the constantly evolving customer environment, ensuring more adaptive and responsive protection against threats.



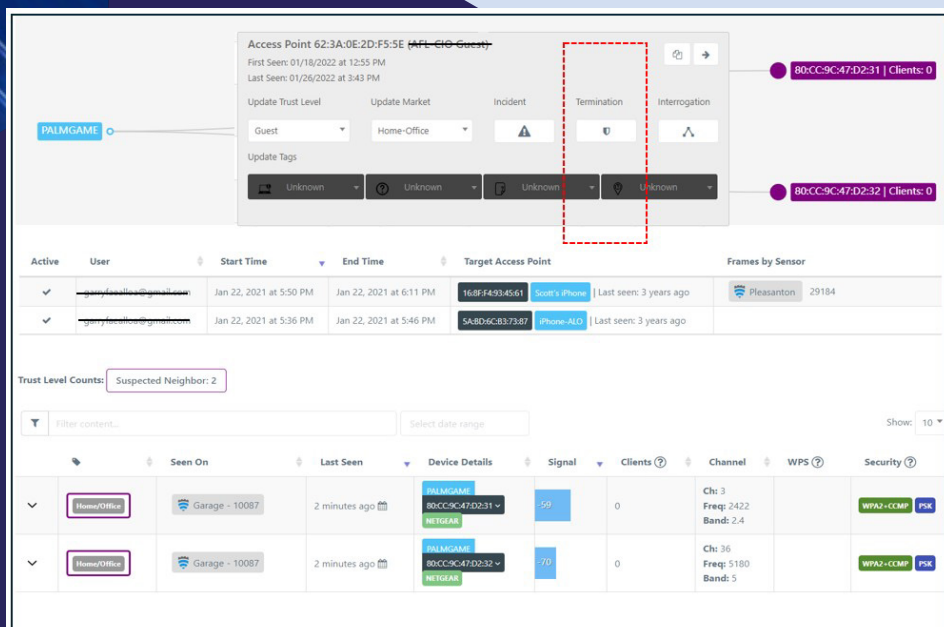
Our patented method of using AI/ML to collect and demodulate radio transmissions is effective using our monitor, analyze, and response stack approach.

AirShields' patented seven-antenna board provides visibility into the most commonly used frequencies for advanced wireless threat coverage and detection.



Our innovative antenna board features seven antennae and is designed to gather RF data across various frequencies. This includes cellular 4G/5G, broad-spectrum IoT (300 MHz to 6 GHz), GPS L1, and Wi-Fi 6, 6E. A key feature of AirShield is 'AirTermination,' a function that allows for the de-authentication of authorized clients, providing an added layer of control and security.

AirTerminate any Unauthorized Devices or Behaviors



Access Point 62-3A:0E2D:F5:5E (APL-CIG-Guest)

First Seen: 01/16/2022 at 12:55 PM
Last Seen: 01/26/2022 at 3:43 PM

Update Trust Level: Guest | Update Market: Home-Office | Incident: [Warning] | Termination: [Off] | Interrogation: [On]

Update Tags: [Unknown] [Unknown] [Unknown] [Unknown]

Active	User	Start Time	End Time	Target Access Point	Frames by Sensor
✓	[Redacted]	Jan 22, 2021 at 5:50 PM	Jan 22, 2021 at 6:11 PM	168F4934561 Scott's iPhone Last seen: 3 years ago	Pleasanton 29184
✓	[Redacted]	Jan 22, 2021 at 5:36 PM	Jan 22, 2021 at 5:46 PM	5A8D9C837387 iPhone-ALD Last seen: 3 years ago	

Trust Level Counts: Suspected Neighbor: 2

Seen On	Last Seen	Device Details	Signal	Clients	Channel	WPS	Security
HomeOffice Garage - 10087	2 minutes ago	80CC9C47D231 NETGEAR	-59	0	Ch: 3 Freq: 2422 Band: 2.4		WPA2-CCMP PSK
HomeOffice Garage - 10087	2 minutes ago	80CC9C47D232 NETGEAR	-70	0	Ch: 36 Freq: 5180 Band: 5		WPA2-CCMP PSK

Wireless Airspace Defense for Critical Infrastructure and Emergency Services.



Broad Spectrum Threat Detection:

Utilizing an SDR (software-defined radio), AirShield can detect, assess, and mitigate a wide range of IoT threats within the 300MHz to 6GHz Spectrum. This includes LorWAN, Zigbee, Zwave, 4G/5G rogue cell towers, GPS jamming/spoofing attacks across L1 satellite connections, and threats in WiFi 2.4GHz—6GHz, including the new 6E standard to detect rogue access points and more.



Advanced Machine Learning:

AirShield employs enhanced machine learning for asset discovery, classification, and behavior analysis. This is achieved through Auto Encoders, ZCODE with NGAM for Wireless Deep Packet Inspection, ensuring high accuracy with minimal false positives.



Extensive Coverage Area:

Each AirShield sensor provides threat protection for up to 25,000 sq ft.



Offensive Pen-Testing Features:

AirShield includes capabilities for offensive penetration testing, such as WPA cracking and IP-based vulnerability assessment.



LTE Back-Haul Connectivity:

AirShield uses LTE back-haul for internet access, completely independent of the production network.



Patented Wireless Zero-Trust Architecture:

This architecture provides a robust framework for secure wireless communications.



Comprehensive Wireless Attack Library:

AirShield has extensive capabilities for detecting a wide range of wireless attacks from Man-In The-Middle, WPA cracking, rogue cell tower detection, and EMI power fingerprinting to prevent layer 0 attacks via the supply chain.



External Attack Surface Management:

The platform offers wired attack surface management features, including IP-based network asset discovery, OS fingerprinting, protocol dissection, open port discovery, and services, all managed from a single AirShield sensor.



Fake Cell Tower Detection:

The system can identify and report the BTS presence of fake cell towers across 3G/4G and 5G Networks.



Cellular Device Spectrum Monitoring:

AirShield continuously monitors the cellular device spectrum for UE detection using PEAK-SPECTRO(TM) - AI UE behavior fingerprinting.



Advanced GPS Detection and Reporting:

AirShield decodes various satellite signals, monitors for deviations in location/time (indicating spoofing or meaconing), and reports changes in state like signal loss, lock, jamming, and spoofing. This information is presented on a centralized cloud dashboard and can be forwarded to third-party platforms via a notification and API system. The dashboard also shows epoch-based histories and the overall health of GPS AirShields.

AirShield -AI smart sensors offer the industry's first AI/ML wireless threat detection platform for next-generation security whereby the 'unseen' invisible threats could infiltrate from layer 0, layer 1, or layer 2 - BEFORE AN IP is assigned.



What is the Response?

- Interrogate Target Access Point
- Isolate Access Point from Client Connectivity
- Physically Track and Remove Devices with LOCH's Incident Application



What is the Policy?

- Define Rules based on Observed Events
- Define a Policy when Rules are Met
- Activate Notification and Response on Triggers



What is the Threat?

- Signature and Heuristic Anomaly Detectors
- AI/Machine Learning based Anomaly Detectors
- Trust Level and Behaviour Monitoring



What is the Source?

- Machine Learning Modulation Detection
- RF Signal Detection and Collection
- Codecs and Protocol Dissectors

INVISIBLE THREATS. VISIBLE PROTECTION.