LOCH TECHNOLOGIES

Invisible Threats, Visible Protection

CAPABILITIES STATEMENT

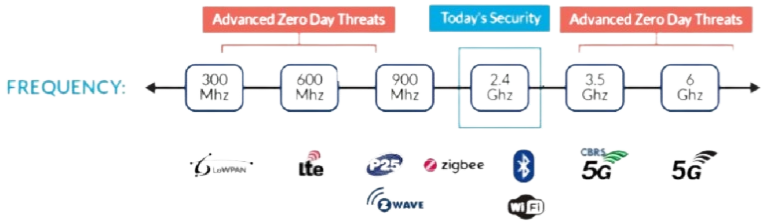
1285 66th Street,
Emeryville, CA 94608
www.loch.io
Company Tel : 888-725-9434

Primary Contact:
Garry Drummond, CISSP, CWNA, CWSP
Direct Tel: 510-703-6149
gdrummond@loch.io

Wireless Airspace Defense for 5G, IoT, GPS , Bluetooth & Wi-Fi

With 80% of devices wirelessly connected, wireless is the new network and new attack surface - creating a massive security blind spot

Today's wireless and RF technologies, including the imminent 5G, pose a significant security challenge for networks and organizations. LOCH's Wireless Airspace Defense™ platform provides advanced threat intelligence across 5G, IoT, CBRS, GPS/Satellite, Bluetooth, and Wi-Fi, offering comprehensive wireless and RF discovery, risk analysis, and remediation capabilities. The AirShield(™) solution, utilizing software-defined radios, monitors 24/7 wireless and RF emissions from 100MHz to 6GHz, providing unparalleled insight and protection.



Differentiators

- Single pane of glass to manage wireless threats across a broad spectrum of wireless frequencies (100 Mhz to 6Ghz)
- Early Warning System - detecting threats before they hit the wired network
- External Attack Surface Vulnerability Management - detect and identify open ports, services and applications before exploitation
- Enforce Zero-Trust Policies and "No Phone" Zones
- Deployable in air-gapped environments - on premise or cloud installations

Gartner COOL VENDOR 2020

Core Competencies

- Software defined programmable radios to detect broad-spectrum RF threats across
- 100 Mhz to 6 Ghz
- Comprehensive classification of all assets in the environment and continuous Intrusion Detection / Zero Trust enforcement
- Wireless Security Threat Research for rapid anomaly detection
- Decoding of all wireless operating systems and protocols including cellular CBRS, IoT. Bluetooth, GPS L1,L2 and Wi-Fi 6E
- Zero-Trust Policy Enforcement
- Rogue Cellular Tower and Stingray Detection
- API integrations for threat mitigation & remediation with RunZero Vulnerability Assessment, Wigle.net for darkweb wireless analysis, SHODAN for wired WAN IP darkweb analysis

PAST PERFORMANCE $15M FOR CYBERSECURITY

1. AFRL Direct to Phase II ($1.8M), Resilient Adversarial Machine Learning, Starting Date: August 2024.
2. NAVY SBIR Phase II ($1.8 M) (August 22- July 2025) – Autonomous Protection for Unmanned Maritime Autonomous Architecture (UMAA)Services.
3. US Air Force: Department of Defense $5M contract (April 2023 – April 2024) for Enhanced Cybersecurity Sensors to detect threats in near and far field emissions.
4. US Army Phase II ($2 M) (November 2019- December 2021) – Tactical Cyber Immune System
5. AFRL and US Army STP Project ($1.5 M) (Nov 2019- Nov 2021) – Autonomic Security Operations Center (ASoC) for OT and Industrial Control Systems.
6. US Army Materiel Command (AMC) project ($400K) to develop a commercial product, AMC Security Operations Center as a Service (AMCaaS).
7. US Navy SBIR Phase I and Option Phase ($237K, starting July 2021- October 2022): Autonomic Protection for Unmanned Maritime Contract Number: N68335-21-C-0555.
8. US Army CERDEC STTR Phase II ($1M, December 2019- December 2021): Tactical Cyber Immune System.).
9. US AFRL and Army Technology Transition Project ($1.5 M, September 2019- September 2021): Autonomic Security Operations Center (ASoC).
10. AFRL SBIR Phase II ($750K, Sep. 2016 – Nov. 2018): Autonomic Monitoring, Analysis and Mitigation (AMAP), Contract Number: FA8750-17-C-0279
11. ONR STTR Phase I ($150K, Jun. 2018 – Dec. 2018): Multi-Layer Mapping of Cyberspace - Contract Number: N68335-18-C- 0416
12. USA CERDEC STTR Phase I ($150K, Aug. 2016 – Feb. 2017): Tactical Cyber Immune System (TCIS), Contract Number: W56KGU-16-C-0065

GPS Spoofing/ Jamming Detection

Rogue Cell Tower / Stingray Detection

Wireless hacking Detection of IoT, Bluetooth, Wi-FI

LOCH TECHNOLOGIES

Invisible Threats, Visible Protection

CAPABILITIES STATEMENT

1285 66th Street,
Emeryville, CA 94608
www.loch.io
Company Tel : 888-725-9434

Primary Contact:
Garry Drummond, CISSP, CWNA, CWSP
Direct Tel: 510-703-6149
gdrummond@loch.io

Wireless Airspace Defense - Invisible Theats. Visible Protection

Patents

- Access Security by Interrogation - # 10,257,226
- Access Security by Interrogation - # 10,764,755.00
- P25 Trunked Radio Vulnerability Management -# 10,999,309
- Zero Trust for Wireless Security - # 11.540,130
- RF Security by Interrogation - # 10,764,755
- Real-Time Interference Monitoring -# 11,595,429
- Behavior Based Monitoring for Radio Frequency - # 11,716,623
- Vulnerability Management, Real-Time Interference - # 11,936,680

Vendor Information

- GSA # G535F01454
- CAGE # 92U44
- SAM # FZPXBVF4UPB
- CMMC #
- NIST #
- DUNS # 05414-6235
- NAICS -541514,541512, 511210, 423430,

Cellular Attacks Detected

- Malicious SMS - attack on mobile-based messaging applications to engage in cyberattacks. Covert data exfiltration is the goal.
- Malware / BOTNETs -stealthy attacks on devices that change behaviour state and data utilization.Excessive data plan usage.
- Fake Cell Towers Detection- protection against rogue base stations and IMSI catchers that lure authorized cellular clients to a fake 4G/5G network for further manipulation.
- Misconfigurations - UE (user equipment) and IoT devices can lead to rogue communications and data exfiltration. Holistic protection for both mobile and IoT.
- SIM Port Swap/Hi-Jacking classify assets using SIM connections to prevent fraud and excessive data plan over billing.

Wi-Fi Attacks Detected

- Rogue Access Points - are connected to an authorized network, usually with an open SSID, allowing attackers to bypass perimeter security for covert data exfiltration.
- Rogue clients - are defined as clients that connect to a rogue or other malicious access point within range of a private network.
- Neighbor access point - are independent networks that are not under administrative control and could be used to bypass internal security controls.
- Ad-hoc Connections - are peer to peer and mesh WiFi, such as Apple AirDrop, between clients that can circumvent security controls and allow clients to evade firewalls and policies.
- Evil twins - are access points mimicking a legitimate AP by spoofing its network to perform data collection, malware delivery and man-in-the-middle attacks.
- Misconfigured Access Points - connected to your private network with a configuration that does not conform to security policies.

IoT Attacks Detected

- Off Network devices - are devices such as spy cameras and drones which do not connect to an approved network but can lead to data exfiltration.
- Shadow IoT - are autonomous networks on non-standard frequencies like 900Mhz i.e HVACs, and Smart Buildings. Existing security tools lack visibility to discover and audit this risk profile.
- Nefarious near-field and far-field covert wireless communications (bugs) - are running on non standard frequencies can lead to data exfiltration.
- CBRS and Private LTE deployments - are non-carrier cellular networks vulnerable to UE and protocol attacks.
- Home / Consumer IoT connected to enterprise networks creating back-door loopholes.

GPS Attacks Detected

- GPS Spoofing: can mislead aircraft regarding their exact positions during takeoff, landing, or taxiing.
- GPS Jamming: Deliberate interference or blocking of GPS signals can cause loss of GPS functionality. . . .Loss or Incorrect GPS Time
- Synchronization: Airport operations interconnected systems (ATC Servers, Ticketing, Baggage Handling, Security, etc.) rely on accurate GPS synchronized time sources to ensure smooth and efficient operations.
- GPS Meaconing - a technique where GPS signal is received and then rebroadcasted with a delay.