Industry 4.0 Solution Brief

Zero Trust Security for Multi-Access Edge

Zero Trust Security for IIoT (Industrial IoT) Wireless Edge

The 4th Industrial revolution (2010 – present) is known simply as Industry 4.0 – the collective initiatives to make our industries, the manufacturing processes and the building and cities we live in smarter. These initiatives are highlighted by the utilization of rapidly evolving technology advances for real-time data collection and analysis to bring efficiency, safety for the citizens and workers, security for processes that deliver critical resources and lastly reduce cost, wastage and the carbon footprint.

Key Business Drivers for Change

- Just-in-Time supply chains with real-time track and trace
- Asset and Location tracking
- Facility, Asset, Fleet and Worker location and contact tracing for safety
- Autonomous or semi-autonomous tools and systems
- Robots and Drones
- Connected and Cognitive networks, machines and devices
- Augmented and Virtual reality
- Artificial Intelligence and Machine Learning
- Computer vision driven quality control systems
- Predictive maintenance solutions
- …and many more

4 Key Questions...

At the heart of the Industry 4.0 revolution is the prolific use of hundreds of millions of IIoT sensors and other devices connected predominantly via a vast array of wireless technologies and protocols.

While IIoT holds the promise to deliver real-time data (monitoring, control, measurement and other analytics), a robust and secure underlying communications infrastructure is at the forefront of all deployment discussions today.

Wireless IoT has created the world's largest attack surface, the scope of which is only broadening with exponential growth in deployment of 5G/LTE. Today's networks and organizations were never built to handle this extraordinary volume, velocity, and hyperconnectivity of IIoT technologies.

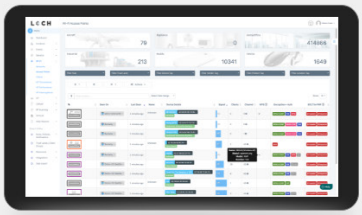
Cyber Threats Impacting Industry 4.0

- Attacks exploiting mobile network vulnerabilities
- Malware via wireless to disable critical infrastructure
- Compromises in supply chain
- Theft of Intellectual Property
- Security breaches involving 3rd Parties

The LOCH Wireless Machine Vision™ platform provides next-generation wireless AI driven threat intelligence across 4G and 5G deployments, broad-spectrum wireless IoT, Citizens Broadband Radio Service (CBRS) as well as 802.11/Bluetooth WiFi environments by providing customers with full IoT discovery, asset classification, risk analysis and actionable remediation capabilities based on a Zero Trust framework.

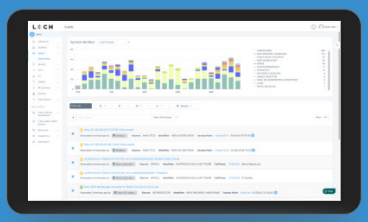
Solution Benefits

DETECT



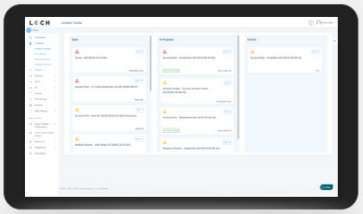
- Detect, identify and classify all broad spectrum RF emitting devices in range
- Device and network pairing communication map analysis and correlation
- Risk assessment threat ranking for Zero Trust network access control
- Mobile App for hunting rogues even if mobile

TRACK



- Wireless deep packet inspection
- Behavioral baselining, analysis and anomaly detection/alerts
- DVR-like capabilities for forensics, including geo-positioning
- Carrier integration with cellular devices for anomaly detection, fraud/ theft and cost management

REMEDIATE



- List and map devices on dashboard or directly into SIEMs.
- Interact with MDM and EMM assets for correlation and feedback on exceptions
- Rectify network segmentation via interactions with SOAR, FW and/or NAC systems
- Automate response and closure via collaboration with ITSM/ITSL and CMDBs

Rogue Cell Tower Detection - Prevent authorized devices from connecting to unauthorised cell towers

Detect and Prevent Evil Twin Attacks - Prevent authorized devices from connecting to unauthorised Wi-Fi Access Points

Roaming - prevent increase in data usage and excessive billing. Monitor potential data exfiltration against traffic base line to flag malware and bots.

Prevent Device Threats - Malware, Firmware Hacks, Sensor IoT Compromises, Man In the Middle Attacks, Device Tampering

Key Differentiators

- **Single pane of glass** to manage ALL wireless threats across cellular 3G/4G/5G, broad-spectrum wireless, CBRS and 802.11/ Bluetooth Wi-Fi devices
- **Early Warning System** - detecting threats before they hit the wired network
- **Edge IoT Vulnerability Scanning** to detect open ports and services to identify exposed threats before they are abused
- **Monitor Enforce Zero-Trust** Policies and "No Phone" Zones
- **Deployable** in air-gapped environments as well
- **API driven integration** with wide ecosystem for automated remediation and collaboration

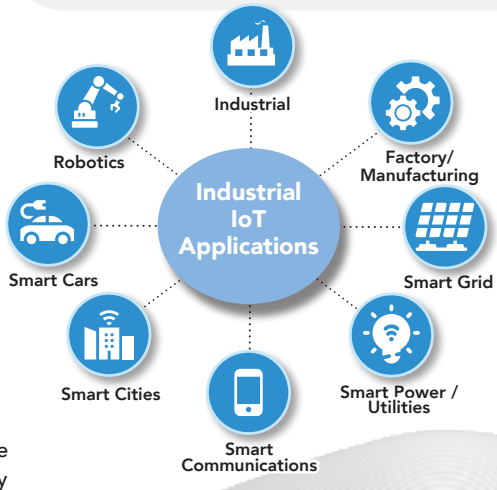
Invisible Threats. Visible Protection

Detect, Track and Secure IIoT devices within your environment

Unique RF in Industry 4.0 Environments

DOMAIN	DESCRIPTION
Instrumentation	IEEE 802.15.4 standards - ISA 100.11a, WirelessHart (IEC62591:2016), IEC 62601, and ZigBee. High performance standards built on IEEE 802.11 - Factory Automation (WIA-FA) IEC 62948.
Wide Area Sensing	LoraWAN and Sig Fox as well as moded of 4G/5G cellular radio standards.
Enhanced Communications	Private LTE: Licensed 4G/5G, Unlicensed UNII3; Shared CBRS
Other Commercial	Satellite, cellular, directional microwave data links, optical (visible light, and land-mobile radio)
Custom Solutions	Radiating coaxial cable and tropo-scatter solutions designed for unique mission criteria needs

Wireless - The new invisible attack surface



LOCH Security for Industry 4.0 IIoT

- **Wireless IIoT Deployments:** In environments where Wireless/RF is used for connectivity, LOCH is the single truth for device inventory. Any device that is emitting an RF signal, will be identified and located..
- **IIoT Security:** Cybersecurity tools that manage such devices are based on network side solutions that use deep packet inspection and protocol dissection of flows from the subnets/VLANs. LOCH's auto discovery will find devices that were missed due to incorrect subnet/VLAN configuration.
- **IIoT Device Scanning:** LOCH solutions includes an 'outside-in', continuous edge vulnerability management solution to provide security validation of devices preventing misconfigurations of open ports, services and threats..
- **4G/5G Security:** In addition to traffic monitoring against established baselines for anomalies, LOCH can sense the presence of adjacent RF channels to thwart man-in-the-middle hijack attempts.
- **LTE Connectivity:** LOCH delivers the ability to monitor traffic from SIMs to alert on excessive use and changes in Device/SIM association.

Security Posture and Operational Efficiency for IIoT Devices

Critical Infrastructure - crucial for delivering essential resources and services. Eliminate threats using broad spectrum RF backdoors.

Sensors – critical for facility, asset and worker safety. Ensure proper network segmentation and block unauthorized access.

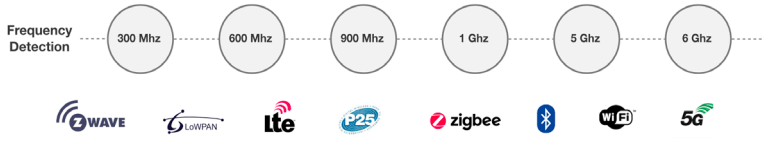
Factory and Process Automation - critical for productivity and efficiency. Ensure network segmentation and unauthorized access.

WiFi USB – Check for all communications into or out of the network for data loss or potential exploitable backdoors for lateral attacks.

Long Range Radio Communications Over Wide Areas – Ensure proper network segmentation and detect hijacked relay stations.

Rogue Cell Towers – Validate 4G/LTE/5G or Private LTE communications for exfiltration and/or malware/process injection.

Network Infractructure – wired and wireless network correlation for misconfigurations that create blind spots for cybersecurity initiatives.



LOCH Core Competencies for Industry 4.0

- Software defined radios to detect broad spectrum RF
- Comprehensive classification of all assets in the environment and continuous Intrusion Detection
- Wireless Security Threat Research for rapid anomaly detection
- Decoding of IIoT protocols
- Zero-Trust Policy Enforcement
- Rogue Cellular Tower and Stingray Detection
- API integrations for threat mitigation and remediation

info@loch.io | 1-888-725-9434 | www.loch.io