WE BRING OUR AI TO SECURE YOUR DATA, TO STOP WHAT OTHERS CANNOT.

The accelerated adoption of digital transformation, with a connected-everything approach, has created another potential target for cyberattacks. IT systems and ICS/OT systems are no longer separate entities, and using different cybersecurity tools for each system is no longer enough to ensure comprehensive protection.

What is ACS (Autonomic Cyber Security)?

An advanced cybersecurity framework designed to automatically detect, respond to, and mitigate cyber threats in real-time. Leveraging AI and machine learning. ACS aims to provide a self-managing security environment that adapts to evolving threats without human intervention.

What is Wireless Airspace Defense

Wireless Airspace Defense is a comprehensive security platform designed to protect wireless networks and devices from unauthorized or malicious activities. This system leverages advanced technologies like software-defined radios (SDRs), AI, and machine learning to provide real-time threat detection, monitoring, and response before a loss or incident occurs.

By melding Wireless Airspace Defense with Autonomic Cyber Security, LOCH Technologies now offers a powerful, innovative solution that provides comprehensive, real-time protection across all network layers, significantly enhancing security posture and operational efficiency for customers.

INTEGRATED DEFENSES KEY BENEFITS

Real-Time Threat Detection

- ACS continuously monitors data traffic and system behaviors to identify potential AI threats and anomalies as they occur.
- ACS utilizes AI and machine learning to analyze any data set to detect anomalies that may indicate an insider our external cyber attack.

Automated Response

- Upon detecting a threat, ACS can automatically initiate predefined response actions to mitigate the impact, such as isolating affected systems or blocking malicious traffic.
- ACS reduces the need for manual intervention, allowing for faster and more efficient threat response.

Adaptive Learning

- ACS learns from past incidents and continuously improves its threat detection and response capabilities.
- ACS can adapt to new and emerging threats without requiring manual updates or reconfigurations.

Minimized Human Error

- By automating threat detection and response, ACS reduces the likelihood of human error, which is often a significant factor in security breaches.
- ACS ensures consistent application of security policies and procedures.

Scalability

- ACS is designed to scale with the needs of the organization, making it suitable for businesses of all sizes.
- ACS can handle increasing amounts of data and growing numbers of connected devices without compromising performance.

INTEGRATED DEFENSES KEY BENEFITS

Real-Time Threat Detection

LOCH's Wireless Airspace Defense platform uses SDRs (software defined-radios) to continuously monitor wireless signals, allowing for immediate detection and response to threats such as unauthorized transmissions, jamming, and signal spoofing.

Comprehensive RF Visibility

LOCH's Wireless Airspace Defense provides visibility across all wireless devices and frequencies within an environment, regardless of their protocol or connection type, helping to eliminate blind spots that attackers might exploit.

Non-Intrusive Monitoring

LOCH's Wireless Airspace Defense employs passive monitoring techniques, ensuring no interference with network operations while enforcing security policies.

Broad-Spectrum Security

LOCH's Wireless Airspace Defense covers a wide range of frequencies, including Wi-Fi, Bluetooth, LPWAN, Private LTE, 5G, CBRS and EMI ensuring comprehensive protection across various communication protocols.

Automated Threat Detection and Response

LOCH'S Wireless Airspace Defense uses AI and machine learning capabilities allowing the platform to automatically detect, assess, and mitigate risks from unmanaged or misconfigured devices-the new external attack surface.

Enhanced Situational Awareness

By continuously monitoring the wireless environment, the LOCH AirShield system provides detailed situational awareness, helping to identify potential security breaches and vulnerabilities

A POWERFUL, INNOVATIVE SOLUTION

By integrating Wireless Airspace Defense with Autonomic Cyber Security (ACS), the value proposition for customers becomes significantly enhanced through a multifaceted and comprehensive approach to cybersecurity.

Comprehensive Security Coverage

End-to-End Protection: The integration offers full-spectrum defense by covering both wireless and wired network vulnerabilities. Wireless Airspace Defense focuses on securing the RF spectrum, while ACS provides data-driven anomaly detection cybersecurity across traditional IT and ICS/OT environments.

Real-Time Threat Detection and Response

The combined platforms enable real-time monitoring and response to threats across all network layers. Wireless Airspace Defense detects and mitigates wireless-specific threats at layer 2 such as unauthorized transmissions and signal spoofing, while ACS handles broader cybersecurity threats through AI and machine learning, from layers 3 and 7.

Enhanced AI and Machine Learning Capabilities

Unified AI/ML Threat Intelligence: Both platforms leverage advanced AI and machine learning algorithms to detect anomalies and predict threats. The unified system provides more accurate and comprehensive threat intelligence by analyzing data from both wireless and wired networks.

Behavioral Analysis

ACS's autonomic capabilities can analyze user and device behavior patterns (BAU), while Wireless Airspace Defense provides detailed situational awareness of the wireless environment. Together, they offer a robust mechanism for identifying unusual behaviors that may indicate a security breach.

Improved Operational Efficiency

Automated Security Operations: The integration allows for automated threat detection, assessment, and mitigation. ACS automates cybersecurity tasks, reducing the burden on IT teams, while Wireless Airspace Defense automates RF monitoring and response.

Scalable and Easy Deployment

Both platforms are designed for ease of deployment and scalability. They can be quickly implemented in various environments, from small enterprises to large industrial IoT networks, ensuring consistent security coverage as the organization grows.

Comprehensive Compliance & Risk Management

Regulatory Compliance: The integrated solution helps organizations meet stringent regulatory requirements by providing continuous monitoring, threat detection, and incident response capabilities. This includes compliance with standards like PCI, HIPAA, NIST, and others.

Risk Management

The combined platforms offer a holistic view of the organization's security posture, helping to identify and manage risks more effectively. This proactive approach ensures that potential vulnerabilities are addressed before they can be exploited.

Enhanced Visibility and Control

Unified Dashboard: Customers benefit from a single pane of glass for monitoring and managing security across all network layers. This unified dashboard provides comprehensive visibility into the security status of all devices, networks, and protocols.

Zero Trust Security Framework

The integration supports a Zero Trust approach to security, ensuring that all devices and users are continuously authenticated and authorized, regardless of their location or network.

By melding Wireless Airspace Defense with Autonomic Cyber Security, LOCH Technologies offers a powerful, innovative solution that provides comprehensive, real-time protection across all network layers, significantly enhancing security posture and operational efficiency for customers.