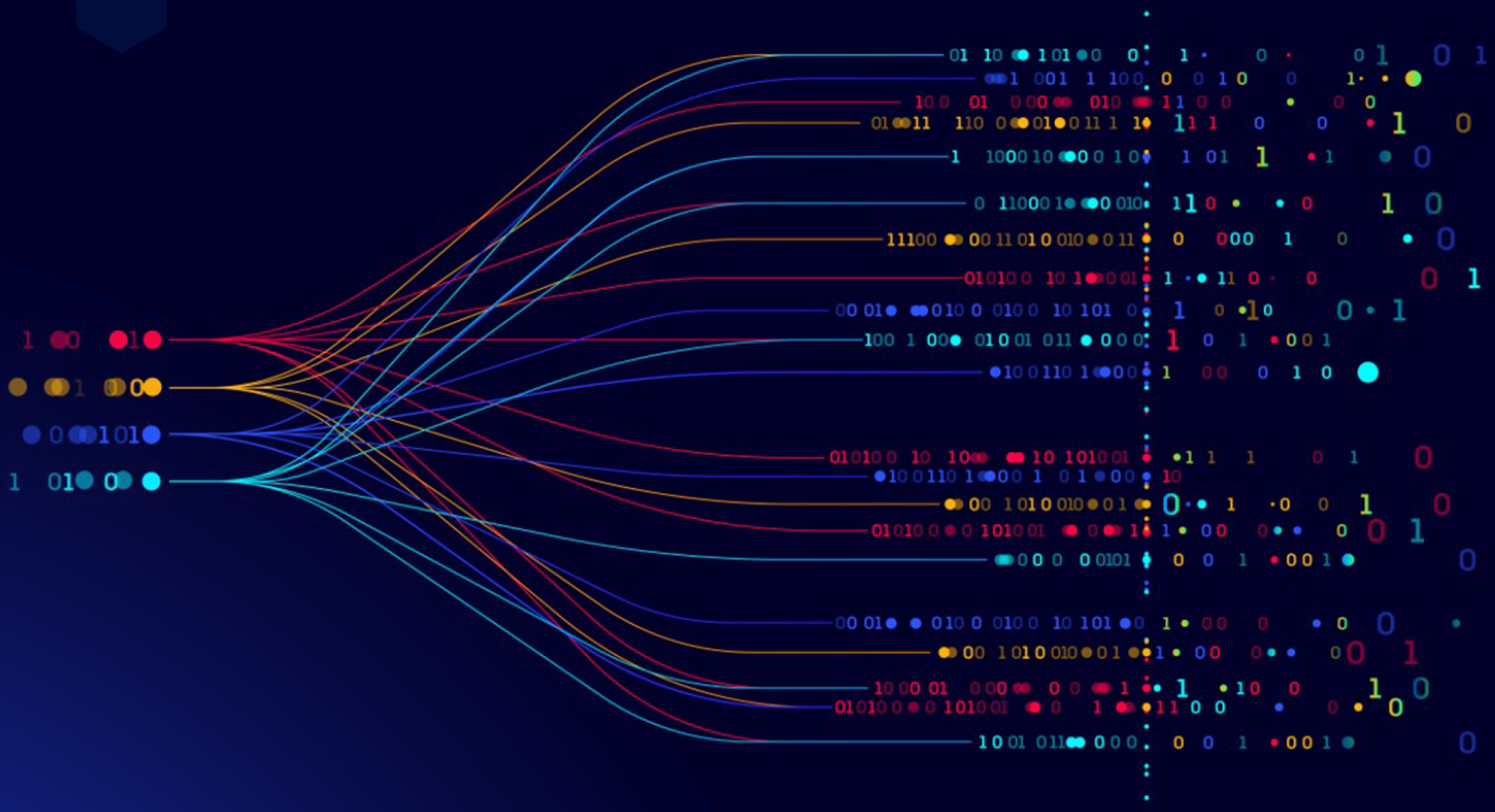
LOCH TECHNOLOGIES

Unlock the Power of Autonomic Cyber Security (ACS): Protecting IT, IIoT, and OT Environments



Predictive Data Anomaly Detection

Autonomic Cyber Security:
Protecting IT, IIoT, and OT Environments

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.

"Autonomic Cyber Security (ACS) from LOCH Technologies, powered by Data Detection and Response (DDR), enables organizations to securely manage the increasing interconnected systems and combat threats to ensure safety, availability, reliability, and resilience. This comprehensive and coordinated approach guarantees security across the entire cyber-physical risk spectrum, including IT, OT, IoT, IIoT, and physical environments."

Professor and Director of the NSF Center for Cloud and Autonomic Computing,
Salim Harini
University of Arizona.

Cybersecurity Challenges in Converged IT and OT Environments: Bridging the Gap for Comprehensive Protection

Digital Transformation Impact:
Accelerated adoption of 'Digital Transformation' has connected everything, significantly expanding attack surfaces in ICS/OT environments.

Convergence of IT and OT:
IT and ICS/OT systems, once separate, are now integrated. This integration eliminates traditional silos but introduces new cybersecurity challenges.

Inadequacy of Disparate Tools: Traditional cybersecurity tools designed for either IT or ICS/OT systems fail to provide comprehensive protection in converged environments.

Integrated Solutions:
There is a critical need for integrated cybersecurity solutions that bridge the gap between IT and OT environments seamlessly. AL/ML Autonomous Cyber Security (ACS) provides anomaly behavior analysis of sensors/actuators, applications, protocols users and comouting resources.

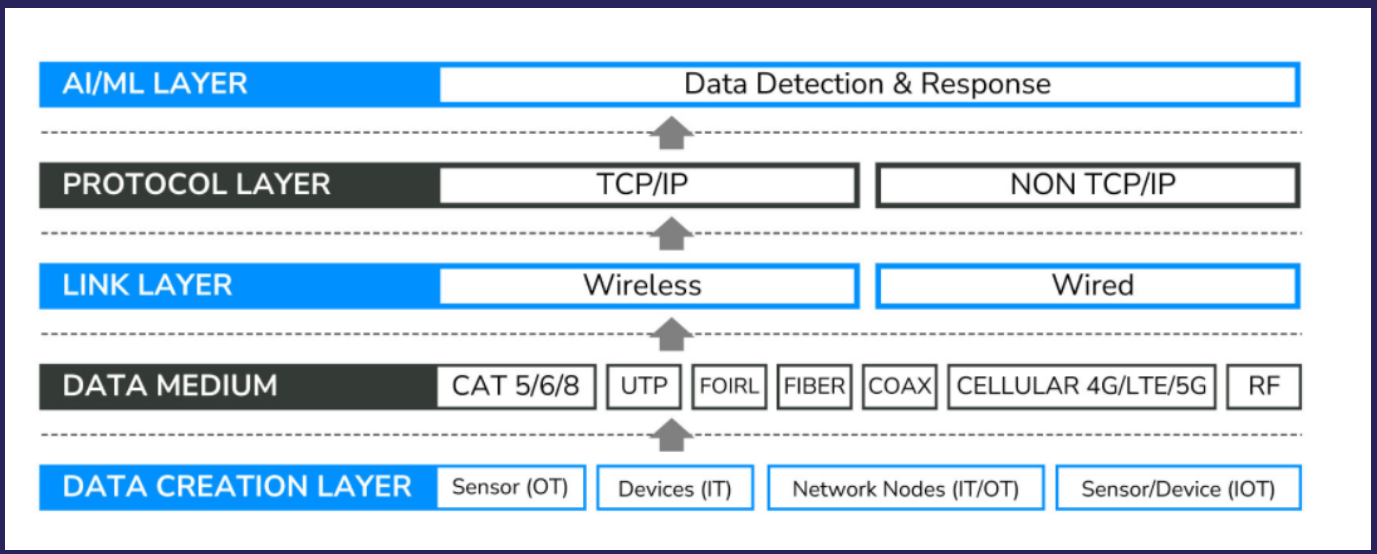
Risk of Cyber Incidents:
Without unified cybersecurity strategies such as AL/ML Autonomous Cyber Security (ACS) organizations face increased risks of cyber incidents that could disrupt operations and compromise safety.

Specialized Security Measures:
Industrial environments require advanced security measures to mitigate risks effectively while supporting ongoing digital innovation.

This format breaks down the problem statement into clear, concise points, highlighting the key challenges and implications for ICS/OT environments.

NetShield: AI Countermeasures You Can Trust to Protect Your Operational Environment

- ML driven Anomaly Detection Methodology by predicting 'datasets'
- Anomalies Detected to thwart zero-day attacks & threats across
  - Sensors Behavior
  - Network Protocol Analysis
  - Identity & Access Validations
  - Network Behavior
  - Applications Behavior



NetShield: Data Driven Detection & Response

Key Benefits of AI/ML Autonomic Cyber Security (ACS)

AI / ML Autonomous Cyber Security (ACS): It functions autonomously, much like the human immune system, providing continuous protection without requiring constant user intervention. This is beneficial as it reduces the burden on users and IT staff to manually detect and respond to threats.

Constant Monitoring and Analysis: ACS continuously monitors and analyzes activities within the network or system. This proactive approach helps in early detection of anomalous behaviors that could indicate potential cyber threats.

Mitigation of Unknown Threats: It addresses both known and unknown threats, including zero-day attacks. This capability is crucial in today's evolving threat landscape where new vulnerabilities and attack methods constantly emerge.

Versatility in Threat Handling: ACS responds to threats regardless of their origin (insider or outsider) or nature (natural or malicious). This versatility ensures comprehensive protection against a wide range of cyber threats.

Independence from User Involvement: Its ability to operate independently from user actions means that it can function effectively even in scenarios where users may not be actively engaged or aware of potential threats.

Advanced AI/ML: ACS aims to provide robust, automated, and efficient protection against cyber threats, enhancing overall security posture while minimizing the need for continuous human oversight and intervention.

LOCH

Key Feature

- Anomaly Behavior Analysis (ABA) of Sensor/Actuator, Applications, Protocols, Users, Network and Computer Resources
- Automated Attack Type Identification
- Autonomic Incident Response based on Attack Ontology

Customer Use Cases

★★★★★

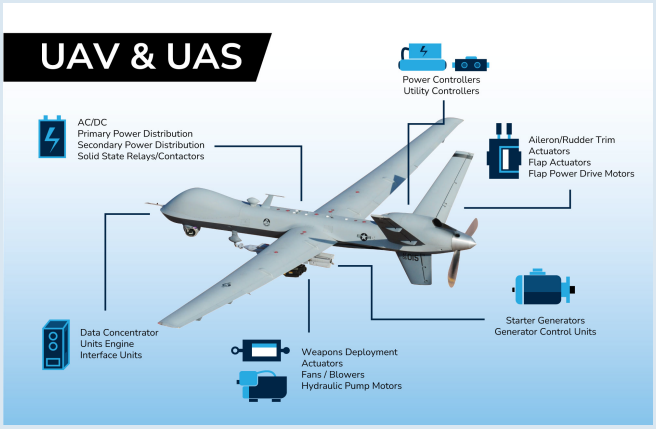
Advantage

- It is based on using AI/ML algorithm to characterize normal behavior that is available.
- It eliminates the manual intensive effort to identify the attack type, and prioritize the response to the attack
- It provides automated approach to characterize the properties of the detected attacks, methods used, vulnerability exploited, and many other relevant properties

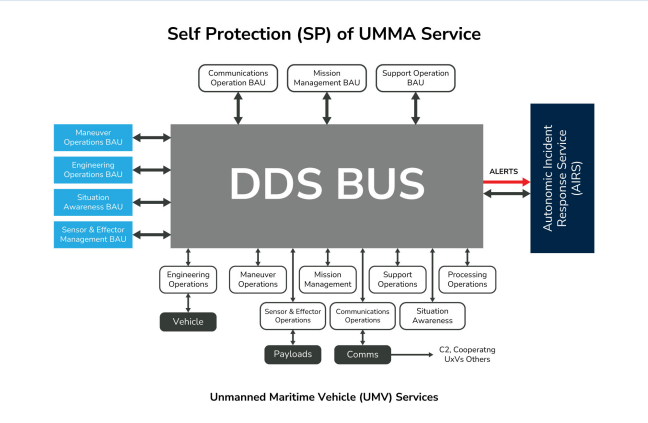
Benefit

- Ability to detect any type of attacks known or unknown. It can be applied to detect accidents/failures that can be trigged by natural or malicious causes
- It can promptly respond to detected attacks to stop them and mitigate their impacts on normal operations
- It provides automated/semi-automated methodology to apply best-practices to respond to detected attacks with little or no involvement of users or system administrators

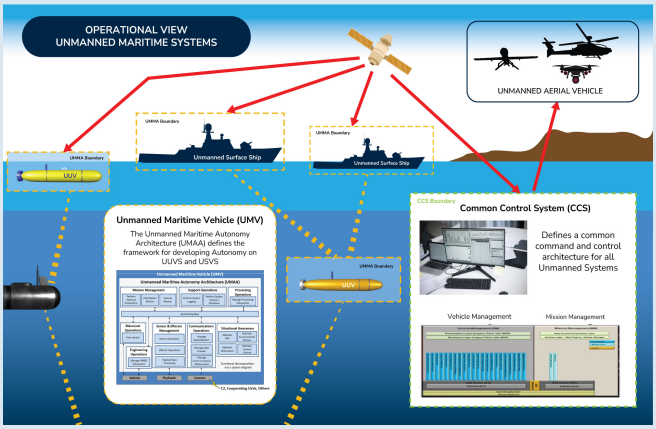
UAV & UAS



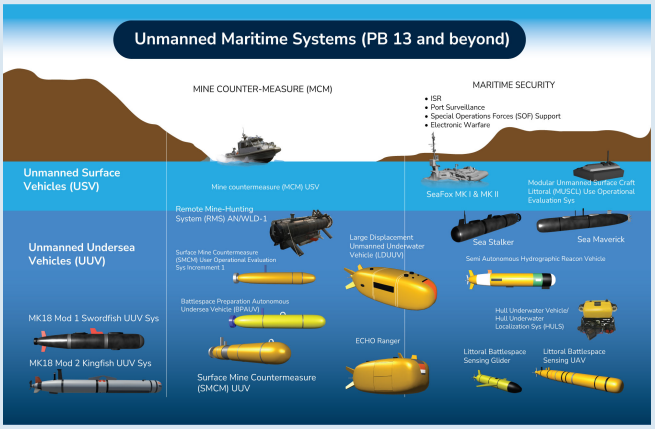
Self-Protection



Unmanned Maritime



Unmanned Surface & Underwater



Airport Command & Control

About LOCH Technologies

LOCH Technologies, Inc. is a global leader in innovative threat monitoring, detection, and mitigation. Our cutting-edge solutions deliver actionable intelligence on every Device, Network, or Thing, empowering organizations to enhance their security posture and eliminate risk.

At LOCH, our mission is to secure and enable the new world of innovation driving the next generation of digital transformation. We are committed to protecting the digital ecosystem, ensuring a safer and more resilient future for businesses and communities worldwide.

To learn more about how LOCH Technologies can help you secure your digital landscape, please visit us at http://www.loch.io