

PROBLEM

As threat levels continue to evolve and become more complex, reliable data collection is imperative for defense readiness. The need for rapid collaboration across the existing system and new cutting-edge system is more critical now than ever for effective domain awareness solutions.

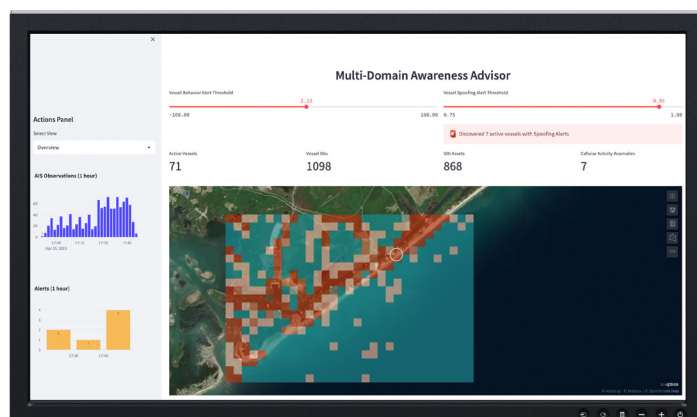
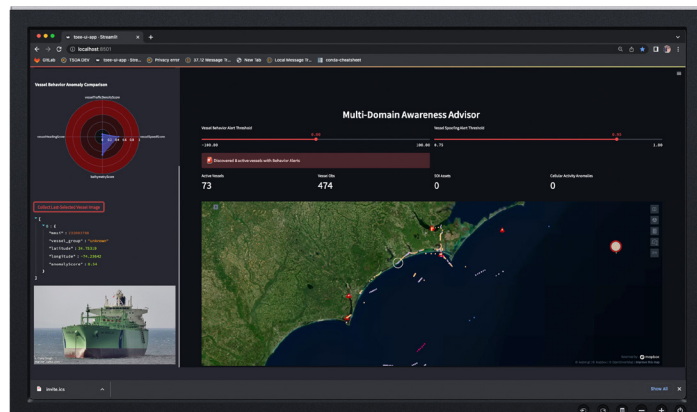
However, these needs are hindered by the proliferation of sensors and excess data quantities that cause a significant strain on operational cognitive loads and bandwidth. This gap adversely affects command timelines and creates uncertainty in the decision-making process across contested multidomain operations. Without effective data processing mechanisms in place, there is a high risk of misinformation.

SOLUTION

Avathon Multidomain Awareness Advisor (MDAA), an application of Avathon's Industrial AI platform, is a scalable artificial intelligence (AI)-based and hardware-agnostic software tool built on a modular technology stack conceived to integrate multi-INT data for use by analysts and warfighters.

MDAA integrates with and enhances existing systems and user interfaces while operating across disparate data types, including textual data sources in multiple languages, multi-physics sensor networks, and multidomain manned and unmanned platforms.

Via normal behavior modeling (NBM), MDAA helps operators achieve decision dominance while shortening Observe, Orient, Decide, and Act (OODA) loops and/or Find, Fix, Finish, Exploit, Assess, Disseminate (F3EAD) cycles. Additionally, it can manage or enhance deployed AI models using Machine Learning (ML) based on battlefield conditions and real-time sensor data backhaul and synthesis while integrating with existing systems.



KEY FEATURES

- *Distributed anomaly detection*
- *Agile software architecture facilitates integration across systems and domains*
- *Compounded impact of orchestrated AI-classes processing across varied data-sets*
- *Relevant alerts indicated to command and control watch-standers*
- *Enhanced domain awareness across echelons in shortened timescales*

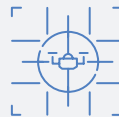
MDAA WORKFLOW





Flexible Deployments

Scalable for use across echelons and across the globe from operations centers, to capital assets, and to the tactical edge to leverage and deconflict classified, unclassified, and commercial data while leveraging existing processes.



Compatibility

Ability to augment hardware sensing platforms with AI domain awareness for more complete target detection and classification.



Awareness and Workflow Enhancement

Enhanced situational awareness and streamlined decision-making achieved by leveraging AI/ML for meaningful anomaly detection, expediting insights and reducing cognitive loads on personnel.



Explainable and Upgradable AI

Supports investigation of insights to eliminate black boxes and model update/management as battlefield information evolves and automates data veracity functionality.



Safeguard Data

Rigorous data protection via zero-day endpoint protection and zero-trust features to ensure trustworthiness and resilience.



Open, Modular Approach

Designed to enhance and augment existing and emergent systems, MDAA is hardware, domain, UI, datatype, and deployment agnostic based on an agile and modular containerized software framework with Kubernetes.

DEPLOYMENT CASE STUDY

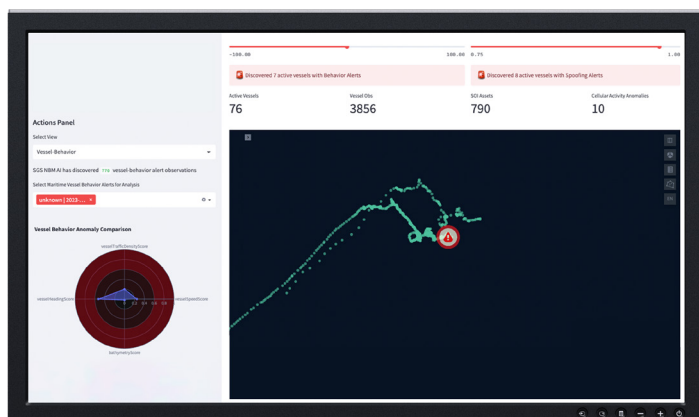
USMC Maritime Recon / Counter Recon

- *Avathon MDAA analyzed 40,000+ electronic signals for abnormal behavior or spoofing*
- *19 vessels were identified as anomalous*
- *Published anomalies with human-readable, explainable AI features on FusedCop*

ABOUT AVATHON

Avathon, a leader in Industrial AI, extends the life of critical infrastructure while advancing the journey toward full autonomy. Avathon's Industrial AI platform empowers commercial and government customers with scalable, secure, and value-driven solutions that enhance efficiency and resilience across heavy industry.

To learn more about how Avathon enables mission readiness, visit avathongov.com.



MDAA analyzing a RedEye-based vessel detection track to generate a vessel-behavior anomaly