Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

NAVAIR Public Release 2022-43

Topic # N193-A01

Advanced Threat Detection and Analysis Using Multi-Dimensional ML for Industrial Control Systems (ICS)

D-Tech, LLC

WHO

SYSCOM: NAVAIR

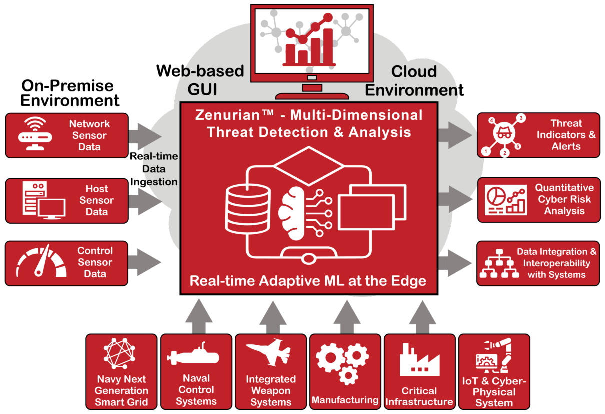
Sponsoring Program: PMA 256 (F/A-18 Program Office)

Transition Target: Navy Smart Grid (NSG), Naval Facilities Engineering Command (NAVFAC)

TPOC:
(301)342-3728

Other transition opportunities: DON: PEO IWS, PEO Ships, PEO UCS, NAVFAC
DOD & Other Federal Agencies: Army Digital Battlefield, SCO/FBI
Commercial Sectors: Critical Infrastructure, Manufacturing, Healthcare, Financial

Notes: Block diagram showing the Zenurian Operational View in Support of Different Programs.



On-Premise Environment

Web-based GUI

Cloud Environment

Network Sensor Data

Host Sensor Data

Control Sensor Data

Real-time Data Ingestion

Zenurian™ - Multi-Dimensional Threat Detection & Analysis

Real-time Adaptive ML at the Edge

Threat Indicators & Alerts

Quantitative Cyber Risk Analysis

Data Integration & Interoperability with Systems

Navy Next Generation Smart Grid

Naval Control Systems

Integrated Weapon Systems

Manufacturing

Critical Infrastructure

IoT & Cyber-Physical System

Zenurian is a Multi-dimensional ML Solution for Adaptive Threat detection and Analytics in Real-Time

WHAT

Operational Need and Improvement: DON and DOD are looking for advanced cyber threat detection techniques to secure their vast mission-critical assets and operational environments. The traditional signature-based threat discovery and intrusion detection techniques are inadequate for advanced persistent threats as the adversaries' tactics, techniques, and procedures are continuously evolving. Zenurian leverages the latest AI/Machine Learning technology to discover anomalies from multiple data sources to identify cyber threats with enhanced accuracy and performance, with little or no human intervention. Designed as a scalable and extensible web-based application, Zenurian provides cybersecurity teams and operation managers with fine-grained continuous monitoring and detection functions to achieve enhanced security management and risk-informed decision-making capabilities. It can be deployed, with minimum integration effort, in both on-premise and cloud environment, to support existing cybersecurity operations, with real-time data analytic performance and cost-effectiveness.

Specifications Required: As a software product, Zenurian is a Linux-based solution and supports a wide range of open platforms adopted by DON/DOD. It operates on commodity computing hardware. All software components are based on DOD-approved open source software. It can be deployed on premise in a single machine or in the cloud in a multi-machine cluster environment.

Technology Developed:
1. ML-driven adaptive techniques and analysis algorithms for anomaly detection and threat identification/analysis
2. Multi-dimensional data fusion and real-time stream processing
3. Extensible and customizable Web platform to support ML for cybersecurity at the edge

Warfighter Value:
1. Real-time cyber threat detection techniques with enhanced performance and reduced cost
2. Adaption to adversaries' tactics, techniques, and procedures
3. Real-time threat alerts and risk-informed decision-making for the operational team

WHEN

Contract Number: N68335-20-F-0568 **Ending on:** October 31, 2021

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Complete Phase II R&D with IV&V	Low	Release of Beta Product after IV&V Test	TRL 5	October 2021
Complete Product Test in a DON/DOD Lab	Med	Obtained Early Adopters and/or Beta Customers in DOD/Commercial	TRL 6	January 2022
Complete Tests in an Operational Environment	High	Identified a Prime and Completed Test for a PoR	TRL 7-8	May 2022

HOW

Projected Business Model: Since the company at this point is R&D focused, our initial strategy with focus on selling the software license and/or IPs. The key is to identify and team up a prime contractor and/or a VAR/OEM vendor as part of the technology transition strategy. In addition, we plan to work with other system integrators and technology vendors through partnerships via product integration with existing cybersecurity tools and applications. This will allow us to embedded our technology within the cybersecurity technology ecosystem, and reach a broader customer base for future growth. Our short-term market strategy also includes:
1. work with prime contractors to help identify potential early adopter programs
2. obtain R&D partners to assist in further verification and validation of the technology to a wide range of applications
3. look for equity investors who understand Zenurian's potential and can help scale product development and accelerate Zenurian's growth

Company Objectives: Our long-term goal is to make D-Tech a leader in real-time ML-driven data analytics, as the ML market is expected to grow continuously in the future. Our short-term goal is to market Zenurian as an ML-at-the-edge product for real-time applications. By working with our partners and advisors, we will identify beta customers and/or early adopters in the DOD cybersecurity marketspace and bring Zenurian to operational readiness in support of different platforms. We plan to participate in various events hosted by STP and their partners, and jumpstart our marketing and outreach effort as we continue improving the product quality and meeting customers' mission requirements.

Potential Commercial Applications: In addition to cybersecurity application across multiple sectors, Zenurian can be easily extended and customized to support many commercial applications, including predictive maintenance in infrastructure and manufacturing, patient monitoring in healthcare, and fraud detection in financial applications.

Contact: Nick Duan, CTO
nduan@dtechspace.com (703) 574-5837