Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
NAVSEA #2022-0353

Topic # N19A-T012
Unified Logging Architecture for Performance and Cybersecurity Monitoring
Altron, Inc.

WHO

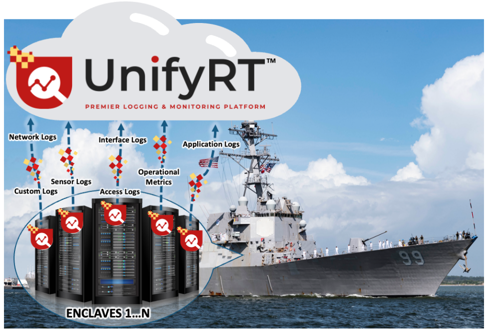
SYSCOM: NAVSEA

Sponsoring Program: PEO IWS (IWS-5)

Transition Target: AN/SQQ-89 A(V) 15

TPOC: (202) 781-4233

Other Transition Opportunities: Government, prime contractors, and commercial partners seeking a solution to rapidly build a data foundation to enable monitoring, cybersecurity, machine learning and artificial intelligence capabilities. The architecture supports extensibility with mobile device and IoT systems and leads to future research in this area. This product also fills a major market gap in residential network/device data collection to enable home automation applications to present homeowners with a simplified understanding of their home network security posture.



U.S. Navy photo by Mass Communication Specialist 2nd Class Anderson W. Branch/Released, Public domain, via Wikimedia Commons

Notes: UnifyRT™ can be used as a unified logging framework for integration with combat control systems, health systems, connected vehicle systems, autonomous vehicles, home networks, and home automation systems. We have recently started working with the Army to develop a novel portable and pluggable data collection hardware device targeted for the Army's armament usage data collection using UnifyRT™.

WHAT

Operational Need and Improvement: The U.S. Navy has an operational need for a unified logging architecture that supports collection, aggregation, storage, and analysis of system performance and cybersecurity logs, events, and alerts produced by Naval Control Systems (NCS). The challenge is that NCSs are comprised of systems of systems divided into enclaves (e.g., Hull Mechanical and Electrical, Combat System, etc.). NCS enclaves generally collect logs at an individual node level, with the log file specific to the events on that node only. Logs are not shared among the enclave or across enclaves. Across enclaves, analysis of NCS performance and cybersecurity monitoring is typically conducted at the system or sub-system level, resulting in implementation differences, incompatibility between monitoring systems, and the inability to produce a full view of the NCS status. UnifyRT™ improves upon existing capabilities providing a flexible, extensible, and platform agnostic unified logging architecture that addresses these needs.

Specifications Required: This novel technology provides a data foundation to build a Security Information and Event Management (SIEM) compliant data architecture that enables the ability to perform correlation, visualization, monitoring, and workflows. This includes collection and storage of data for network traffic to provide the ability to track network activity and visualize network gaps. It collects all data needed to construct a performance and cybersecurity monitoring dashboard that displays who is logged in to the system, file and executable access, connected devices as well as any other security use cases.

Technology Developed: UnifyRT™ provides robust data ingestion, enrichment, transport, aggregation, and storage of system log data across enclaves into a central repository. UnifyRT™ simplifies the ability to seamlessly create a data foundation to enable performance monitoring, cybersecurity, machine learning and artificial intelligence capabilities. This technology equips NCS Engineers with the ability to identify, analyze, and correct system-wide problems during development, integration and production events. UnifyRT™ serves as a distributed streaming platform providing publish and subscribe to streams of data, storage of data in a fault-tolerant manner, and processing of streams of data as they occur.

Warfighter Value: This novel real-time plug and play unified logging system reduces staffing required to manage the logging stack, reduces product training costs, supports developer subsystem debug and analysis, makes adding and managing data sources extremely easy, and supports performance/cybersecurity data retention.

WHEN

Contract Number: N68335-21-C-0268

Ending on: Feb 24, 2023

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Integration and Test of technology prototype in relevant environment	Low	Successful prototype validation in an AN/SQQ-89 lab environment	4	3rd QTR FY20
Integration and Test of technology prototype in lab environment	Low	Successful prototype validation in an AN/SQQ-89 relevant environment	5	3rd QTR FY22
Prototype Demonstration	Low	Successful Demonstration and test in an AN/SQQ-89 lab environment	5	4th QTR FY22
Integration and Test of technology prototype in operational environment	Low	Successful prototype demonstration of more mature technology in AN/SQQ-89 lab environment	6	1st QTR FY23
Technology Seminal Transition Event	Medium	Logger deployment, data aggregation and test conducted in an operational environment	7	3rd QTR FY23
Seminal Transition Event	Medium	Successful integration and qualified test event	8	3rd QTR FY24

HOW

Projected Business Model: Our core business strategy is based on selling technology & services to support Automated Testing, Integration, and Monitoring (ATIM™). A foundational part of this model is data collection and aggregation using UnifyRT™. UnifyRT™ is the core of a suite of products being developed to support our ATIM™ model. We are in the process of developing two other products, UnifyRT™ Insight™ and UnifyRT™ Hive™. UnifyRT™ Insight provides an interactive user interface that employs rule-based and machine learning analytics to automate root cause identification and monitoring of system issues. UnifyRT™ Hive™ is a novel portable and pluggable data collection hardware device targeted for the Army's armament usage data collection for AI applications and targets commercial markets such as vehicle health management and monitoring of connected vehicles and transportation edge devices.

Company Objectives: Expand the deployment of the UnifyRT™ suite of products to other government systems, prime contractors and commercial entities to deliver ATIM™ solutions.

Potential Commercial Applications: UnifyRT™ is a flexible logging framework that can be integrated with any type of system from autonomous vehicles to home automation. UnifyRT™'s innovative administration tool provides an intuitive user interface that eliminates the complexity of the underlying logging stack so that government users, commercial users, or even homeowners can easily perform aggregate logging of devices and services associated with their systems or on their network.

Contact: Mike Gercken, Vice President, Engineering and Technology Solutions
mike.gercken@altroninc.com (843) 984-9369