Department of the Navy SBIR/STTR Transition Program

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.
SPAWAR SR-2017-294

Topic # N132-140
Utilization Of Inference Engine Technology For Navy Cyber Situational Awareness
La Jolla Logic, Inc

WHO

SYSCOM: SPAWAR

Sponsoring Program: SPAWAR PEO C4I PMW 130

Transition Target: Navy Cyber Situational Awareness (NCSA)

TPOC:
(619)221-7810

Other transition opportunities: Widely applicable across government and commercial markets as a stand-alone product, or integrated enhancement to existing systems. Potential Navy transition opportunities include legacy tactical networks, as well as cloud. The technology is applicable across all classification enclaves with potential to assimilate multi-level threat data using a cross domain system (CDS).

Notes: Intelligent Situational Awareness for Advanced Cybersecurity (ISAAC) augments exiting malware detection tools by identifying novel patterns worthy of further analysis. This approach provides a layer of evaluation beyond the current detection tools which seek to identify 'known bads'.

WHAT

Operational Need and Improvement: The operational need for ISAAC technology is undeniable. As a nation, the ever emerging cyber threat must be kept in check through a battery of tools and techniques addressing all layers of the IP stack and all mission domains. Within the DoD, the application is for land, sea, air and space - all canvased and dependent upon the cyber domain. ISAAC identifies 'novel' components on network before threats ever materialize.

Specifications Required: This technology uses an artificial intelligence and machine learning approach to detect anomalous system behavior, indicative of a cyber breach. Beyond registered threats, that is those that have been previously identified, ISAAC is tuned to seek out and identify unregistered threats, also know as zero day or potential zero day threats.

Technology Developed: The technology developed recognizes and establishes patterns of behavior to determine a baseline of 'normal' and identifies variance from the baseline. Applied to the cybersecurity domain, ISAAC contributes to the cyber situational awareness picture through use of automation and machine learning. The system identifies 'known good' entities to determine which items are novel and require further analysis to determine if 'known good' or 'know bad'; current techniques typically identify only 'known bad' entities. Behavioral anomaly detection is a key aspect of the solution.

Warfighter Value: ISAAC will improve warfighting capability by improving the security posture of DoD networks and system, protecting the information domain to ensure more reliable, accurate and available systems and data. Beyond cybersecurity, ISAAC understands system behaviors and has broad applicability across system-of-system in any context where understanding behaviors of complex systems is needed. For example, in comparing warfighting capabilities of complex integrated systems across shipboard platforms to achieve maximum predictive lethality.

WHEN

Contract Number: N00039-16-C-0061 **Ending on:** April 10, 2017

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Requirements Definition & Code Development	Low	System definition and theory complete, code compiles and passes modular testing (completed)	TRL 3	January 2017
Developmental Test & Evaluation	Med	Charts and graphs produced to demonstrate outcome of code testing represents theory (completed)	TRL 4	March 2017
Accreditation and Network Integration	Low	ISAAC received an Interim Authority to Test (IATT)	TRL 5	April 2017
Operational Test & Evaluation, Initial Fielding	Med	System trained and producing findings	TRL 7	May 2018

HOW

Projected Business Model: Leverage DoD SBIR funding to address technology risk in development, pursue commercial investment in furthering beyond lab risk to full rate production. Business model includes IP protection and productization through other large commercial entities, as well as continued developmental funding through venture capital and use of company internal research and development (IR&D).

Company Objectives: Develop and prove out technical approach through DoD initiatives. Pursue follow on commercial financing to bring to sustained Commercial Off-The-Shelf (COTS) product. DoD leverages unlimited use rights. Objective is to productize and transition the capability to both DoD and global commercial markets.

Potential Commercial Applications: Technology is readily applicable to other cybersecurity objectives beyond cyber situational awareness, including the efficiency of current malware detection products. Foundational, underlying capabilities have wide applicability beyond cybersecurity, such as to reduce computational efforts application to big data processing. Beyond cybersecurity, using artificial intelligence and machine learning has applicability to better the understanding of system-of-system behaviors when complex interactions are in play. ISAAC observes interactions which results in raining, with no prior awareness (unsupervised learning), and applies that learning to monitor activity and detect anomalies.

Contact: Stacey Anfuso, Principle Analyst
sanfuso@lajollalogic.com 6195596083