Department of the Navy SBIR/STTR Transition Program

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

ONR Approval #43-8761-21

Topic # N192-131

Persistent AI based Threat Detection (PAIT)

Perceptronics Solutions, Inc.

WHO

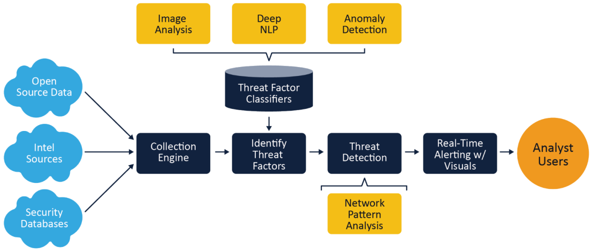
SYSCOM: ONR

Sponsoring Program: Minerva INP

Transition Target: Naval Maritime Command and Control Operations Center, Marine Corps Information Operations Center, U.S. Army Training and Doctrine Command

TPOC:
Dr. Allen Moshfegh
allen.moshfegh@navy.mil

Other transition opportunities: Force Protection organizations and Intelligence Community analytics



Notes: Builds on the OssaLabs computational social science toolset (www.ossalabs.com) Collaborating with K2 Solutions Inc. (K2SI.com) to incorporate warfighter expertise in high threat environments

WHAT

Operational Need and Improvement: SECNAV INSTRUCTION 3300.2C - Commanders should give special emphasis to reducing the vulnerability of personnel, family members, resources, facilities, and critical infrastructure under DON cognizance to terrorist acts

Specifications Required: A multidimensional machine learning and reasoning system that incorporates trend and sentiment analysis techniques and algorithms into a range of entity and behavior analytics for integration into a shared-networked environment for timely intervention and neutralization of harmful intents

Technology Developed: The PAIT system uses the power of artificial intelligence including machine learning to detect emerging threats and intent to harm by monitoring open source and security-related data sources. Information on potential threats as well as their associations is collected and synthesized from both structured and unstructured data. A library of machine learning-based classifiers that each search for different specific kinds threat factors (i.e., evidence of intent to harm). Each threat factor classifier is highly specialized and thus able to achieve very high accuracy without supervision. Multi-faceted machine learning techniques underly the threat factor classifiers and are used to examine all aspects of available data including text (using advanced NLP and deep-learning embeddings), image, temporal behaviors, and relationships. Patterns of threat factors that exist across the network of relationships are examined to “connect the dots” between disparate pieces of evidence and identify important threats

Warfighter Value: PAIT provides timely and relevant information to Force Protection personnel enabling the reporting and dissemination of information on threats

WHEN

Contract Number: N68335-20-C-0837 **Ending on:** September 9, 2022

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Complete primary algorithmic components	Low	Benchmark core text classification and image analysis algorithms against known data sets.	4	3rd QTR FY21
Fully integrated prototype	Low	Demonstration of data ingested, analysis including machine learned threat factor detectors are applied to data, results are rendered to user through user interface.	5	2nd QTR FY22
Exercise participation	Med	Use prototype in support of military training exercise where open source data is being analyzed to identify threats	6	3rd QTR FY22
Complete enhanced prototype	Med	Based on feedback from exercise, improve prototype performance and ready for evaluation	6	4th QTR FY22
Insertion with end user	Med	Insert prototype into transition partner environment and integrate with their data sources	7	TBD

HOW

Projected Business Model: Provide an open scalable software framework for AI-based multidimensional-trend analytics and learning methods that can exploit behavior analysis techniques and provide insight into threating behaviors. PAIT capability is being integrated into the commercial software product OssaLabs Version 4.0

Company Objectives: Provide artificial intelligence solutions to reduce cognitive overload with automated force protection and intelligence processing. Search vast amounts of data, reliably identify suspicious behavior in isolation, and recognize patterns of those behaviors to identify threats

Potential Commercial Applications: Commercial threat management and workplace violence prevention services

Contact: Timur Chabuk, Vice President, Machine Learning and Advanced Analytics, Perceptronics Solutions
timc@percsolutions.com 571 235 5720