Topic: N162-115

Star Lab Corporation

Warden: Cyber Threat Anomaly Detection for Combat Systems

Star Lab's Warden is a minimally invasive technology designed specifically to detect advanced cyber threats inside unique defense compute environments, e.g., systems running customized Linux and real-time operating systems. Consisting of a lightweight sensor package, an ensemble of detectors, and an artificial neural network, Warden identifies potential cyber threats and reports them via the syslog mechanism. Warden's functionality has been prototyped, tested, and verified using realistic test and training environments for the Aegis Weapon System. Star Lab, an embedded systems security company, is dedicated to protecting devices and systems operating in open, hostile environments. Our goal is for prime contractors to integrate Warden as they modernize combat systems to defeat never-before-seen cyber-attacks.

Technology Category Alignment:

Autonomy
Networks and Communications
Assuring Effective Missions
Resilient Infrastructure
Trust Foundations

Contact:
Adam Fraser
adam@starlab.io
(202) 706-7027
https://starlab.io/
SYSCOM: NAVSEA
Contract: N00178-18-C-7002

Corporate Brochure: https://navystp.com/vtm/open_file?type=brochure&id=N00178-18-C-7002

Department of the Navy SBIR/STTR Transition Program

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

NAVSEA #2018-0643

Topic # N162-115

Warden: Cyber Threat Anomaly Detection for Combat Systems

Star Lab Corporation

WHO

SYSCOM: NAVSEA

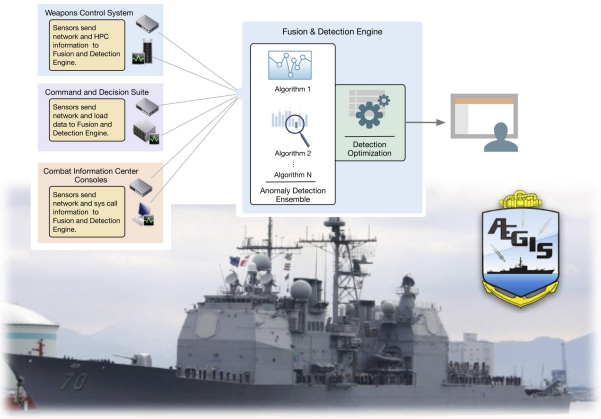
Sponsoring Program: PEO Integrated Warfare Systems (IWS) 1.0, AEGIS Integrated Combat System

Transition Target: AEGIS

TPOC:
(540)284-0035

Other transition opportunities:
Integrated Maritime, Ground, and Aerial Combat Systems

Notes: Warden is designed to use data captured by several sensor modalities such as network sniffers, logs, and load monitoring software. Warden includes a fusion and detection engine where an ensemble of detectors identifies deviations from a baseline model. Warden also includes a collection of detectors to identify deviations from baseline models. Warden's Ensemble Framework includes sensitivity controls in the form of detection optimization algorithms to reduce false positives. This is particularly important, as false alarms quickly erode operator trust.



WHAT

Operational Need and Improvement: Cyber-attacks against mission-critical combat systems are a growing concern across the Department of Defense. Combat systems are comprised of subsystems running customized Linux and real-time operating systems, enterprise intrusion detection systems and security products. A threat detection system is required to address gaps in weapon system security such as the inability to (1) detect undocumented attacks, (2) operate without impacting real-time constraints of modern combat systems, and (3) rapidly detect attacks while also achieving a low false positive rate.

Specifications Required: The threat detection system should be capable of being integrated with any hardware and software system. The system should provide real-time detection of imminent, undocumented cyber-attacks while also having no impact on system message latency or application performance. The system should identify cyber-attacks using data collected through network traffic, computer usage logs, and load monitoring software. False alarms should be minimized.

Technology Developed: Warden consists of a lightweight sensor package that monitors combat system behaviors, e.g., communication patterns, application performance statistics, application control-flow statistics, etc.; an ensemble of detectors to identify cyber threats, in particular, undocumented attacks delivered by the advanced persistent threat (APT); and reasoning algorithms in the form of an artificial neural network to verify malicious activity. Warden's minimally invasive sensors and efficient, highly-reliable algorithms detect attackers attempting to access or tamper with and alter combat system software/firmware, and they severely limit an attacker's freedom of maneuver if access is obtained.

Warfighter Value: Star Lab's novel technology applies anomaly detection to unique combat system operational environments for the purpose of cyber threat detection. Warden is minimally invasive allowing it to be integrated with real-time operating systems. Additionally, operators can trust that Warden will detect only real cyber threats as advanced artificial intelligence algorithms are used to reduce the occurrence of false positives. The potential of this technology is so promising Innovative Defense Technologies (IDT) has partnered with Star Lab during the Phase II to support the integration of the technology into the Aegis combat system.

WHEN

Contract Number: N00178-18-C-7002 **Ending on:** December 21, 2018

Milestone	Risk Level	Measure of Success	Ending TRL	Date
Sensor Framework	Low	Combat system degradation no more than 1%	4	October 2018
Detection Ensemble Framework	Med	Detection within 90 seconds of attack with < 1% false positive rate	4	October 2018
Logging and User Reporting	Low	Manual evaluation by AEGIS SMEs	4	August 2018
Deployment and Configuration Interface	Low	Manual evaluation by AEGIS SMEs	5	November 2019
Transition	Med	Prototype demonstration on representative system	5	December 2019
Transition	Med	Prototype demonstration on representative system	6	December 2020

HOW

Projected Business Model: Star Lab's business goal is to license this technology to Prime integrators. Under this business model, Star Lab will provide a flexible perpetual license to its software per a pricing guide to be developed during the later stages of Phase II. Star Lab's product licensing model was purposely chosen to offer the lowest total cost of ownership (TCO) for our customers, compared to the cost of hiring, developing, and maintaining internal security solutions. Unlike many software vendors who are only interested in making a quick sale, Star Lab develops long-term relationships with its customers, typically becoming a trusted security partner across a number of product lines and corporate initiatives. Additionally, Star Lab will offer product support for training, tailoring, integration, and deployment. Star Lab utilizes a straightforward pricing rate per hour for professional support and works with customers to estimate the time needed to transition from initial concept to production deployment.

Company Objectives: In the short term, Star Lab will integrate and transition Warden through its partnership with IDT. During the Phase II and possible Phase III, Star Lab will demonstrate and validate this technology through seminal test events using existing (potentially augmented) system integration test procedures within a test environment provided by IDT. Long-term objectives include leveraging existing anti-tamper / cybersecurity programs across the DoD to developed numerous strategic partnerships with key DoD Prime integrators. Collectively, these efforts strengthen the company's commercialization strategy and provide Star Lab with the proper foundation to bring this novel solution to a wide range of markets.

Potential Commercial Applications: In addition to the defense industry, Warden can be leveraged to protect mission-critical or safety-critical systems in the information technology (IT), manufacturing, industrial, and medical sectors. These systems, like defense systems, are critical to the American way of life. Novel capabilities are desired to prevent costly, and even life-endangering impacts of cyber attacks, from adversaries that leverage undocumented attacks.

Contact: Adam Fraser, COO
adam@starlab.io 202-706-7027