



Navy SBIR/STTR Success



Intelligent Agent Security Module (IASM)

IASM reduces current tests of network analysis by 75%, reduces false alerts by 99%, and improves positive identification of network attacks by 64%.

Topic Number: N99-167

SBIR Investment:
\$2,900,000

Phase III Revenue:
\$34,950,390

Mr. John Mullen
john.mullen@promia.com
(415) 536-1600
101 The Embarcadero, Suite 200
San Francisco, CA 94105

About the Technology:

Promia has developed a high-speed, secure distributed messaging infrastructure that connects agents gathering network information from many COTS, GOTS and Promia sources. This product allows network analysts to see more in their networks than ever before, in order to identify and isolate cyber network attacks. Results are translated into simple English for Navy watch standers and centralized analysts to help them monitor the electronic terrain of their global networks. This product has been put into production at Navy Network Operating Centers, Navy Aircraft Carriers, Navy Fleet Information Warfare Center, Marine Corps Network Operating Center, and Navy SPAWAR Systems Center Labs.

Naval Benefit

This product provides for reduced headcount at the network watch stander and network analyst positions, as the IASM consolidates many current workstations into one console, resulting in a 75% reduction in current tests. IASM provides a 99% reduction in false positive count of network alert messages, providing a much clearer picture of electronic terrain, and provides a 64% improvement in accuracy in identifying network attacks. The system applies various analytic processing techniques such that intrusion patterns can be detected as they occur. Organizations can use the system to detect large-scale intrusions that were previously undetectable, decrease false alarm rates and perform dynamic drill down of intrusions for analysis and determination. The system combines Security Event Information Manager (SEIMs), enterprise network mapping, and network health capabilities for much better network operation awareness and security intelligence. Multiple systems may be deployed and integrated in a grid format to support enterprise wide network operations.

Transition

In 2012, the Navy conducted a review to determine which product would be used to satisfy the Navy portion of a US STRATCOM Enterprise Mapping and Leak Detection (ENMLDS) requirement for all DoD networks. Promia Raven, which is the commercial transition product resulting from the IASM program, was chosen above all others. Based on this decision, the Navy purchased this capability from Promia, and plans to begin the upgrade with 23 existing Promia Raven systems in global Navy Network Operation sites in 2013. To continue the planned Navy-wide ENMLDS deployment, the Navy also ordered thirteen new Raven 2100 Rev B systems and nine more analytic ENMLDS units for new installation in the OCONUS Navy Enterprise Network, supporting Navy bases in Singapore, Guam, Diego Garcia and eight other sites around the world.



Promia, Inc.

Published 2013