



PROMIA, Incorporated
160 Spear Street, Suite 320
San Francisco, CA 94105
<http://www.promia.com>

PROMIA, an established development firm and software provider since 1991, is in the business of providing solutions designed to support highly secure, reliable, scalable and interoperable applications. PROMIA's open-standard solutions comply with the newest emerging security regulations and specifications, providing high levels of information security assurance.

PROMIA has targeted military, government, healthcare and financial institutions, developing sophisticated new intrusion detection tools that employ artificial intelligence techniques on high speed, high volume network systems.

PROMIA POC: John Mullen
415-536-1600
john.mullen@promia.com

Navy POC: Mike Weber
619-524-7333
michael.weber@navy.mil

SBIR Investment: \$953K*

Non-SBIR Investment: \$18.5M

* Includes Phase II Enhancement Funds



Intelligent Agent Security Module (IASM)

About the Technology

IASM is a high-speed secure distributed agent based system operating as a single analytical and statistical processor that connects agents gathering network information from many contractor and government off-the-shelf sources. IASM "watches" network traffic on many levels to determine misuse, fraud, or attack. Information is analyzed at the agent level, then normalized and fused as it is sent to multi-level IASM servers. The data is then correlated and analyzed further to determine cyber attack profiles in real time. Results are translated into simple English for Navy watch standers and centralized analysts to help them monitor the electronic terrain of their global networks.

Benefits to SPAWAR and other DoD Programs

Since the mid to late 90's, the DoD has been subject to an exponential increase in computer-network system threats. Complex computer software, developed in rapidly changing commercial speed to market environments, has unintentionally introduced into user systems several computer-network vulnerabilities. The increasing ability of the cyber threat to exploit vulnerabilities and penetrate computer network systems undetected jeopardizes the war fighter's reliance on computer-network data availability and assurance in mission critical information. Network security administrators have had little ability to analyze the vast amount of cyber reconnaissance, intrusion, and attack data to qualify the security risk of an operational computer-network system. IASM gives the Navy an enterprise-wide security risk situation awareness view. For the first time analytic capabilities can accurately identify, source, and isolate cyber attacks.

Why IASM Provides Improved Security

- Reduces false positive network intrusion alerts to less than 1 percent
- Based on using an intrusion detection system alone, improves identification of network attacks by 64 percent
- Provides accurate and timely situation awareness with better forensic analysis, data reduction, graphic display reporting, and incident response
- Can detect novel non-signature attacks with cluster attack analysis and anomalous intrusion detection
- Reduces watch manning requirement by approximately 80 percent

Military and Commercial Significance

- Thirty-six advanced IASM systems have been delivered to the Navy under a Phase III contract since 2001. These systems have been deployed worldwide in:
 - Fleet Network Operating Centers
 - Navy Component Task Force activities
 - SPAWAR System Center Laboratories
 - Aircraft carriers and Flag command ships
- Commercial versions of the IASM product are available as a security internet appliance.
- The FAA provided funding for a pilot installation.

