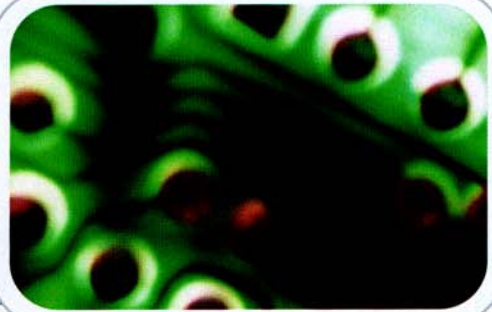


PROMIA, Inc., San Francisco, CA | www.promia.com

2001-2002 NAVY CAP Participant

Success Criteria: More than \$13M in Phase III including Congressional Funding

Promia's Intelligent Agent Security Manager (IASM) gives the Navy an enterprise-wide security risk situation awareness view.



Since the mid to late 90's, and especially since the 9/11 attacks, the Department of Defense (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 user systems to 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 wide operational computer-network systems. Promia's Intelligent Agent Security Manager (IASM), however, 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.

Headquartered in San Francisco, CA, Promia specializes in large-scale, customized, distributed (meaning many computers in the network), high speed, high security network systems for large commercial and government customers. Their products are used in environments requiring high security, high reliability, high performance and scalability. Promia has been a leader in this complex industry since 1991 and counts the National Security Agency (NSA) and a large number of Fortune 250 companies as key customers, including IBM, Chevron, Ford and FedEx. Mostly, these customers use Promia's solutions to keep their valuable networks secure.

In September 2001, Promia received a \$7 Million Phase III award from the NAVY for their Intelligent Agent Security Manager (IASM). IASM, a high-speed secure distributed agent based

system operating as a single analytical and statistical processor, connects agents gathering network information from many contractor and government off-the-shelf sources. IASM "watches" network and host-based 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.

At the time of Promia's transition from the Navy SBIR's Phase II to Phase III, the company was participating in the 2001-2002 Navy Commercialization Assistance Program - CAP (now called the Transition Assistance Program - TAP). The Navy CAP, and its culminating May 2002 Opportunity Forum, provided valuable contacts and promotion for the development of Promia's business. According to John Mullen, President of Promia, in the enterprise security business, promotion is best if it's done quietly or not at all. Mr. Mullen says participation in the CAP provided confirmation that his idea for enterprise security was a good one for implementation in the Navy and provided excellent "quiet" promotional opportunities for Navy applications.

Recently, Promia has received \$3.6 M, then an additional \$3.0 M in congressional funding to modify, test and deliver their advanced technology, this time specifically for shipboard deployment. This continues the Phase III contract and complements a multi-year research and development effort by Promia and the U.S. Navy to design and build and deploy the systems. The IASM is to be deployed as a primary means of providing information analysis and protection on ships and shore-based facilities.