



# PROMIA IASM 5100

**PROTECT · DETECT · RESPOND**



**IASM MODEL 5100**

## Intelligent Agent Security Manager

Under contract to the US Navy, and in cooperation with the National Security Agency, Promia developed and delivered a military version of the Intelligent Agent Security Module™ (IASM) to supplement and enhance the performance of network security products on global Navy networks. In conjunction with that product Promia is now developing a commercial version called the Intelligent Agent Security Manager™.

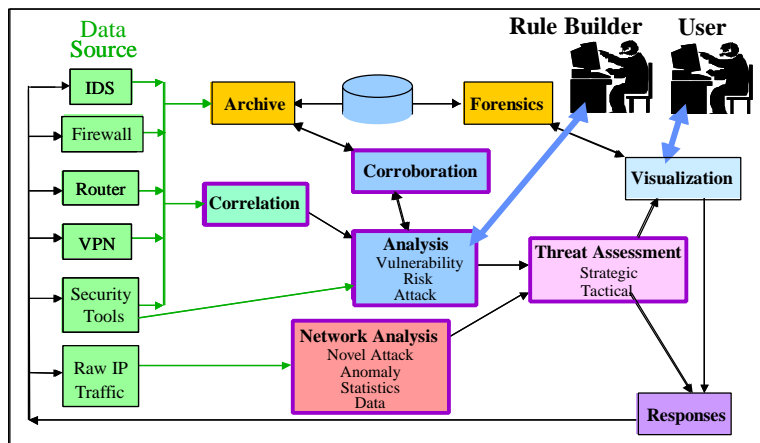
IASM collects data from intrusion detection systems (IDS), firewalls, routers, and virtual private networks (VPN), fuses then analyzes the data using advanced statistical tools, to increase awareness of attacks being conducted against enterprise networks.

The IASM system utilizes multiple advanced approaches to solve the problems with the current commercially available IDS products and recently emerging correlation-based systems. The technical approach taken is fundamentally different in that the design is based upon automating the network intrusion analyst process instead of advancing the means to analyze attack signature data. To achieve the goals of the program, a combination of knowledge engineering, fuzzy systems, statistical analysis, and computer systems engineering are used. In this manner, the objectives of false alarm reduction and novel attack detection can be accomplished while reducing the manpower required for monitoring and administering enterprise mission essential networks.

statistical analysis, and computer systems engineering are used. In this manner, the objectives of false alarm reduction and novel attack detection can be accomplished while reducing the manpower required for monitoring and administering enterprise mission essential networks.

IASM provides unique capabilities to consolidate data from security products deployed on a network and provides intelligible reporting to the operators. The IASM network and forensics information provided can be utilized by staff with varied skill levels, ranging from minimum networking knowledge to experienced security analysts.

Figure 1 is a functional diagram showing how all of the component functionalities relate to each other in IASM. Unlike the development practices for many products in this area, the Navy first determined that these capabilities are needed, and then set about building a system with all of these capabilities. The emergent technologies mentioned earlier satisfy different subsets of these capabilities, but none are known to encompass all of them.



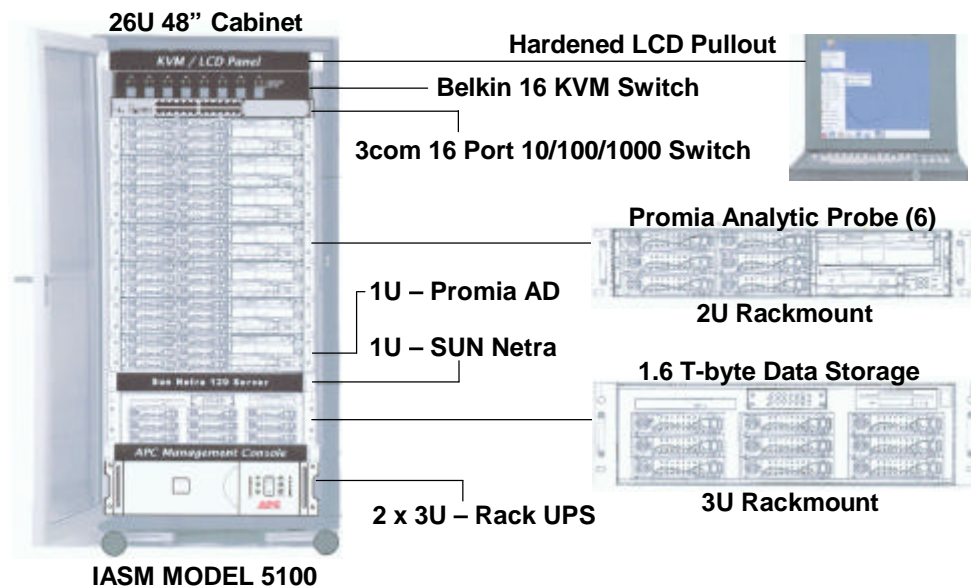
**Figure 1**

Promia has included the ability for analysts to prepare and input their own analytic rules through an ontology editor, allowing the system to reproduce expert human decision processes in critical situations. Designed to be used with the Promia Cyber Warfare Laboratory™, IASM uses the Protégé Knowledge Database as a base for building, editing and storing expert and fuzzy custom rules. Rule Builders develop logic based on human expert knowledge, statistically derived knowledge, and observed behavior from the CWL clean room environment. These are tested offline in the CWL, then included in production IASM operation against cyber terrorist intrusion attempts.

---

## Promia IASM 5100 Hardware Configuration

---



When not in use, the 1U LCD panel / keyboard / mouse unit folds neatly into the rack. When extended, it is used with the 16 port KVM for screen / keyboard / mouse access to the IASM 5100 system machines. The BELKIN PR02 series 15-port KVM centralizes control over the computers in the IASM 5100 cluster. The 3com 24-port 10/100/1000 fast switch delivers the necessary bandwidth and network segment control at speeds up to 1.0Gbps. The 6 Promia Analytic Probes each contain dual Intel Pentium-III 1.40Ghz processors with 133 MHz FSB, 512K L2 cache with 2.0 Gbyte fast DDR memory, 2 Broadcom-5702 1.0Gigabit Ethernet NICs, and 2 80Gbyte 7200 rpm, ATA-133 IDE removable DASD. These form a cluster unit for distributed analytic processing of potential threats to the network under protection. The Promia AD (Anomalous Detector) is an IP protocol anomaly engine at Gbit speeds. The hardware configuration is identical to one of the Promia Analytic Probes. The SUN Netra provides compatibility to Solaris based systems in customer environments. The Disk Storage Unit is comprised of dual Intel Pentium-III 1.40Ghz processors with 133 MHz FSB, 512K L2 cache with 2.0 Gbyte fast DDR memory, 2 Broadcom-5702 1.0Gigabit Ethernet NICs, 8 x 160GB 7200 rpm ATA-133 IDE drives and an 80Gbyte 7200 rpm, ATA-133 IDE for system kernel. Each system drive is independently channeled to a high performance, 64-bit based 3ware 7500 PCI IDE controller capable of reading 180MB and writing 127MB per second. This is used to store long periods of information for extensive historical forensic analysis.



### Promia, Incorporated

info@promia.com www.promia.com

160 Spear Street Suite 320  
San Francisco, CA 94105  
(415) 536-1600

322 Commons Way  
Princeton, NJ 08540  
(609) 252 1850

839 Elkridge Landing Rd Suite 211  
Linthicum, MD  
(410) 694 0322

1490 Drew Ave., Suite 180  
Davis, CA 95617  
(916) 756 0884