

# Intelligent Agent Security Manager™

*Full life cycle incident management*

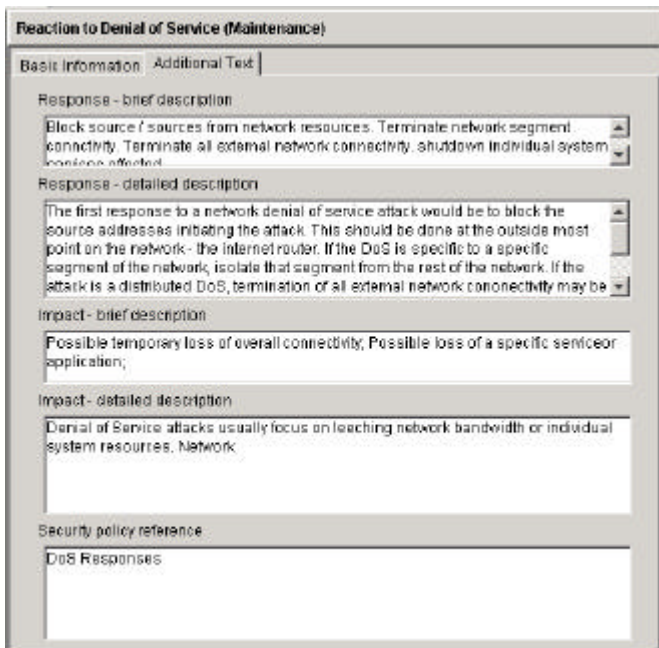
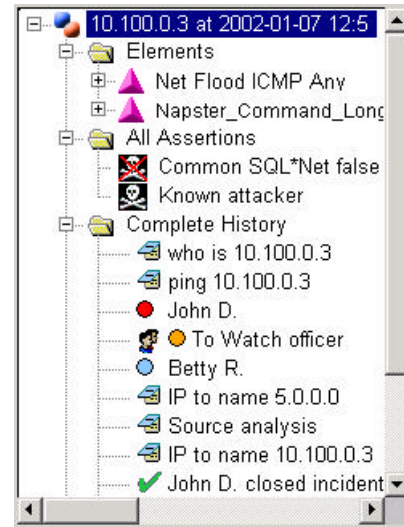


**Promia, Inc.**

Protect • Detect • Respond

## Incident Handling

IASM provides integrated incident management allowing operators and analysts to work seamlessly together to resolve issues. With just a few clicks, common operator tasks such as who is, country of origin, ping, and trace route investigations can be performed and stored in the incident folder. Commentary can be added and outstanding questions flagged for visual queues that other team members can then provide answers to. In a 24x7 environment such teamwork and workflow management is critical to sustaining network security. The initial priority is automatically assigned based on the customer's incident policy and threat level. Incidents can be further prioritized and assigned with just a few mouse clicks. The incident folder tracks all the interactions and response action results in a comprehensive manner. This tracking also allows continuous evaluation of IASM settings and performance characteristics.



## Response Recommendation

IASM automatically provides a list of possible responses. These responses can take a variety of forms including textual guides, e-mails, source investigation, firewall interaction and both offensive and defensive measures. Any response must be considered along with its impact on operations and other factors. IASM permits the customer to define the criteria and policy for responses based on their needs and objectives. The behavior may even be conditional based on threat level. Unlike other applications, IASM provides several interfaces for third parties and customers to build custom responses.

### Outcome Tracking and the IASM Knowledgebase

Most reported incidents are not one off occurrences. IASM meets the requirement of tracking the results of incident response. IASM does this transparently as personnel interact with the application. This knowledge is then immediately shared among the security team members and can be then queried in the future.

*Have we seen any incidents like this in the past?*

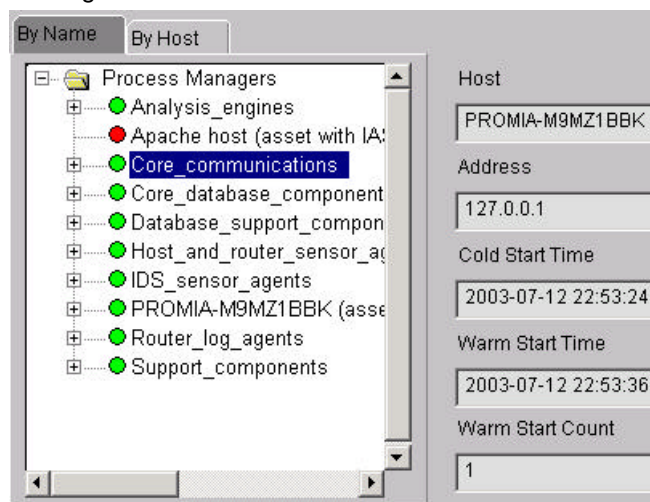
*Was it a false positive?*

*If not, what did we do and which responses were successful?*

IASM provides quick access to these questions and others using the IASM knowledgebase. With security operations running 24x7x365 and the movement of personnel, the enterprise can not afford to lose this critical knowledge.

### Security Health Monitoring

IASM includes numerous features to monitor the status of itself and its collaborating security devices. This includes remote monitoring and management of IASM components. Alert record retrieval is controlled in real-time to maximize throughput and correlation effectiveness. A spike in one alert log is automatically managed by IASM and shown visually for personnel.



### Security from the Hardware Up

IASM is built upon a robust security centric infrastructure. The most secure application infrastructure though is of no use if it resides on an insecure or untrusted environment. This includes the operating system and the surrounding applications. Security applications installed via CD possess this fatal trait. Unlike other security managers, IASM is delivered on hardware that has undergone stringent security hardening and review. In fact, Promia helped the U.S. Department of Defense (DoD) to develop the Linux hardening scripts.

IASM uses strong SSL encryption and authentication among its components. Unlike other applications, IASM uses the field proven internationally implemented open standard **Common Object Request Broker Architecture (CORBA)** for its communication and security. This open standard enables disparate applications to securely interoperate at high speeds with granular security. The IASM resource access rules can even be defined to limit access to objects and to specific operations on those objects. As a longstanding member with the Object Management Group (OMG), Promia helped define the CORBA Security model. Promia then jointly developed a reference implementation with the U.S. National Security Agency (NSA). This proven open standard is now widely being used for its scalability, robustness, and speed. In fact, the CORBA standard is part of the U.S. IT 21 initiative.