

Intelligent Agent Security Manager™

Full life cycle incident management



Promia, Inc.

Protect • Detect • Respond

Forensic Analysis and Reporting

IASM includes an extensive set of querying and reporting tools. The IASM status reports provide critical real-time network-wide situational awareness. Unlike other security management applications that use third party canned packages, the IASM tools are very aware of the network security domain. The IASM reporting macro language includes numerous network centric functions among its hundreds of functions. Besides a full report designer, a comprehensive set of ad hoc query tools are provided ranging from free form to point-and-click querying. This breadth of tools is required by the very nature of security analysis. Many investigative actions are repeated, but other actions are more ad hoc, possibly looking across time, space, and databases.

The screenshot shows three windows from the IASM interface. At the top is the 'Task Bar Reports - FIWC' window, which contains a tree view with folders for 'Task Bar Reports', 'Summary Reports', 'Detail Reports', 'Alerts List Report Cybarlab', and 'Incidents that are open with details'. Below this is the 'Incident 070204-0 - FIWC' window, displaying incident details for ID 070204-0 with a high priority. The 'Property' table shows:

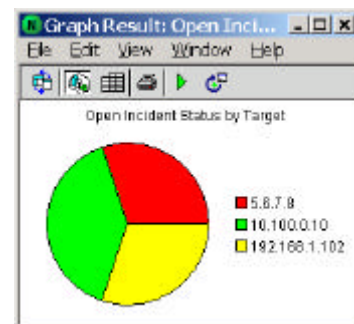
Property	Value
*** Summary ***	
Event Type	CoincidentEvent
Event ID	210703-0
Created	10/7/2002 12:52:32 PM
Issue	10.100.0.3 at 2002-01-07
Alert Count	2
*** Network ***	
Enclave	FIWC
Source IP	10.100.0.3
Source Port	

At the bottom right is the 'Report Viewer: Open Incident Summary Reports' window, displaying a 'Shift Turnover Summary Report' with the following data:

High	Priority	Time	Assigned to
High	1023.03	11:53:07	Watch officer
Issue:	IOS Telnet Buffer Overflow		
Source:	1.2.3.4.80		
Target:	5.6.7.8.8080		
Underlying alerts: 1			
<input type="button" value="Details..."/>			
High	10702	12:50:29	Assigned to: Incident handler
Issue:	Same source IP		
Source:	23.45.67.89.80		
Target:	192.168.1.102.0000		
Underlying alerts: 3			
<input type="button" value="Details..."/>			

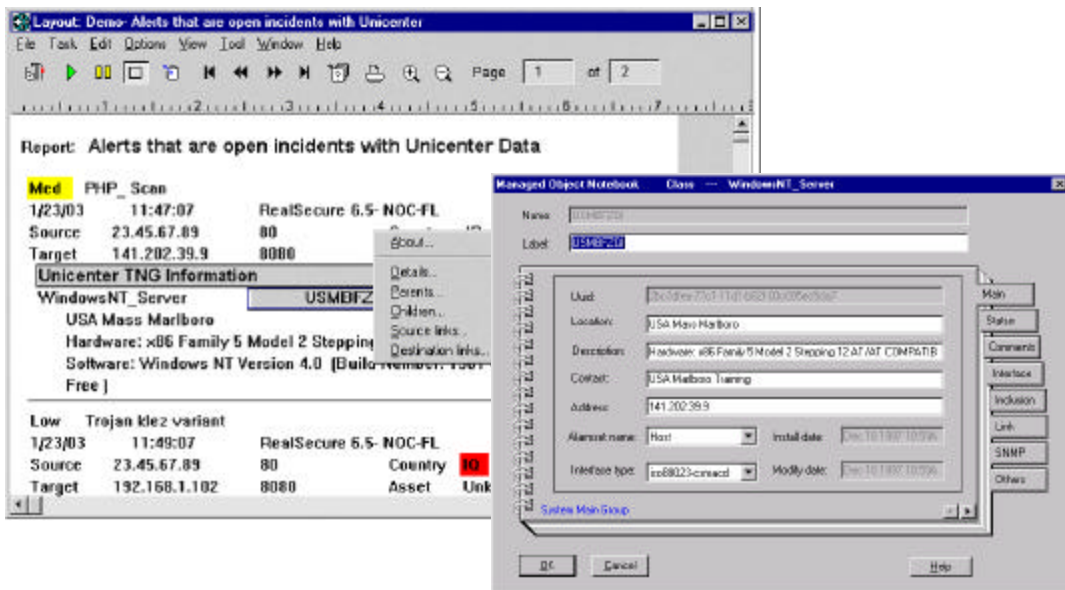
Graphs, Hot Buttons and More...

IASM reports can include graphs with numerous charting options. Besides drill down capability, reports can even include hot buttons that, when clicked, open up the main IASM Incident Management window itself. If you see an interesting incident shown in a report, the details are just a click away. No more writing down long ID's and retyping them. Reports are now fully interactive and a complete part of the overall investigative process. As a result, managers, analysts, and operators can better understand outstanding issues and accomplish their tasks more productively.



[Easily Join Security Data with Other Enterprise Data](#)

Unlike other applications, IASM is not limited to accessing SQL databases. In fact, IASM permits access to non-SQL databases using a set of customer proven data source drivers. Reports can be easily created that join across heterogeneous data sources, servers, and data formats. Combining log alert data with enterprise asset information or other data is quick and easy. In addition, an optional Computer Associate's Unicenter TNG interface permits joining security data with Unicenter TNG data. This interface has gone through the Unicenter certification process and takes advantage of the comprehensive Unicenter WorldView API.



[Enterprise Security Portal](#)

In addition to the comprehensive desktop components, IASM also provides a full web application server function. This allows customers to schedule, publish, and distribute security reports such as shift turnover and management reports. The IASM web application server is used to rapidly build security portal applications that take advantage of IASM's rich feature set. Customers are not locked into a vendor installed browser centric applications. IASM even includes built-in exporting of Adobe Acrobat PDF, rich text format (RTF), hyper-text markup language (HTML), and other common formats.

