Promia Raven 1100 Appliance

The Raven 1100™ Appliance: Security Operations Management And Situational Awareness For The Most Demanding Networks

The Promia Raven 1100 is a hardened Security Asset, Event, and Incident Management appliance that was developed to meet the operational and security requirements of the U.S. Navy on its Carrier-class ships. The Promia Raven 1100 appliance is a small, 1U, half-depth hardware device that hosts the Promia Raven Management, Analysis, Repository, and Sensor components.

The Management component includes features for: identifying site-specific appropriate policy-driven responses, incident validation, and incident closure (after operator remediation of the problem), as well as the secure web-based Promia Raven 1100 user interface for accessing those features.

The Analysis component has algorithms to detect operational and security incidents that would not otherwise be visible from any single sensor. These algorithms use a unique combination of expert system and statistical aggregation and correlation techniques to analyze events from multiple sensor sources. An additional result of the Analytic algorithms is a natural language description of each incident detected.

The Repository component consolidates and stores the logged event records from many commercial NIDS, HIDS, firewalls, VPN appliances, routers, host operating systems, and software applications into a unified online repository. The event records are actually collected, filtered, and forwarded by intelligent Promia Raven software agents that are placed at strategic locations on the network.

Finally, the Sensor component directly monitors network traffic to both detect known attack signature patterns and passively identify, fingerprint, and map network assets. It uses an enhanced Snort engine to compare network packets with “Bleeding Edge” Snort rules that have been developed by the Snort community and independently tested by Promia. The Sensor component includes filters that use local knowledge to eliminate false positive events, aggregate consecutive instances of the same event, and filter events according to white- and black-lists of IP addresses. It also retains annotated instances of the packets that match Snort signature patterns for later remote forensic review by skilled incident analysis personnel.

For more information, please contact:

PROMIA, Inc
160 Spear Street, Suite 320
San Francisco, CA 94105

415-536-1600 (Phone)
415-536-1616 (Fax)
sales@promia.com

www.promia.com

Promia Raven 1100 Appliance

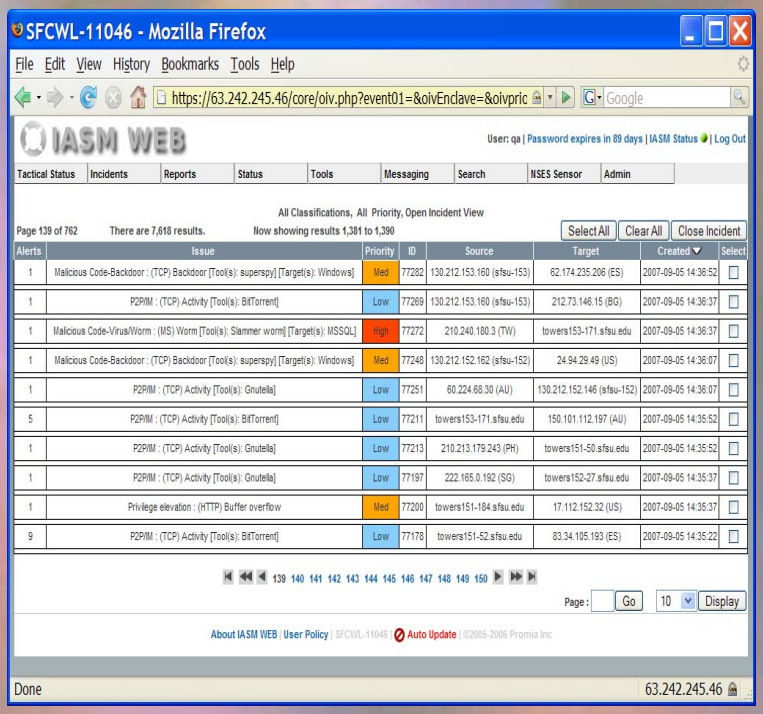
Operations-Oriented User Interfaces

The Promia Asset Viewer Graphical User Interface

The Promia Raven 1100 comes with the Promia Raven Asset Viewer (AV) GUI, which presents a flexible, powerful, 3-dimensional, consolidated visualization of all assets and incidents on the monitored network. The AV shows versions and patch levels of node operating systems, device and application status, ports in use, and other related information. The AV provides a real-time tactical status view of the Promia Raven 1100 incidents and the operational status of the Promia Raven 1100 appliance – as shown in the diagram to the right.

The Promia Incident Management Web User Interface

In addition to the Asset Viewer, the Promia Raven also provides a web interface for viewing and managing incidents, assets, and the appliance configuration options. Using the web interface, an operator can drill down into and close incidents, see different tactical status views of detected incidents, generate reports, manage all features of the Promia Raven appliance, set up users and peer Promia Raven appliances, check for and install Promia Raven appliance updates, and download the Asset Viewer installer.



For more information, please contact:

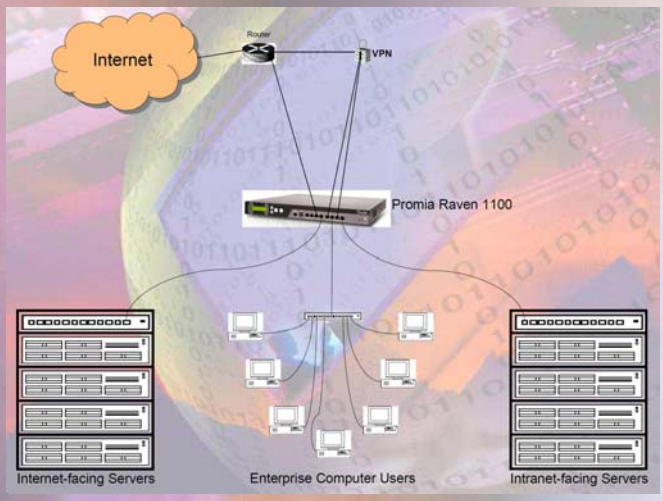
PROMIA, Inc
160 Spear Street, Suite 320
San Francisco, CA 94105

415-536-1600 (Phone)
415-536-1616 (Fax)
sales@promia.com

Promia Raven 1100 Appliance

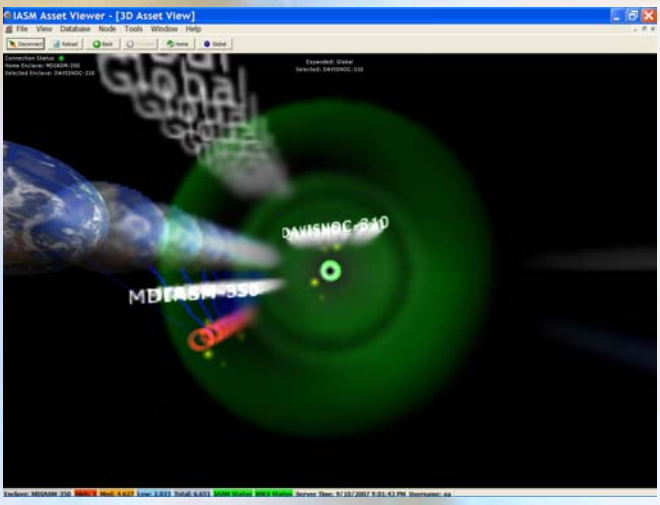
Scalable Enterprise Security Management

The Promia Raven 1100 Appliance is designed to provide security operations monitoring and management for a departmental or branch office of a large enterprise. As such, it is designed to monitor and manage 1-3 network segments that are physically co-located: as shown in the diagram, to the right. Promia Raven 1100 Appliances, however, are even more effective when deployed to multiple departments or branches and then linked together into a unified security operations and management system.



Promia Raven 1100 appliances are designed to interoperate with each other in both hierarchical and peering architectures. Once configured for interoperation, the Promia Raven 1100 appliances exchange information about incidents they have detected and their current operating status. The Promia Asset Viewer shows all of the appliances to which the current appliance is connected in its Global View.

The Promia Asset Viewer uses a “warp” effect (shown in the picture to the right) as its unique visual cue that an operator is navigating from the Global View to a remote Promia Raven 1100 appliance. During the “warp” the AV logs into the remote device to retrieve its asset and incident information for display in the usual fashion. The “warp” capability thus enables any combination of distributed or centralized network security operations management.



For more information, please contact:

PROMIA, Inc
160 Spear Street, Suite 320
San Francisco, CA 94105

415-536-1600 (Phone)
415-536-1616 (Fax)
sales@promia.com

Promia Raven 1100 Appliance

Promia Raven 1100 Appliance Technical Specifications

Case	1U rack mount – 427mm (deep) x 458mm (wide) x 44 mm (high)
Processor	IA86 64-bit, multi-core
Memory	4GB SDRAM
Disk Storage	750GB
Interfaces	• 3 USB 2.0 ports • 1 RS-232 console port • 6 RJ45 10/100/1000Mbps Ethernet ports for 3 in-line monitored networks • 1 RJ45 10/100/1000Mbps auxiliary Ethernet port for reserved for future use • 1 RJ45 10/100/1000Mbps uplink Ethernet port for management
Power	100-240 VAC, 50-60 Hz, 8.5 amp
Capabilities	**Network Intrusion Detection Sensor:** Signature-based, uses Snort rules; **Passive Asset Detection Sensor:** Passive detection of assets and network topology; **Active Asset Detection Sensor:** Active probing of known assets for services; **Security Event Collection:** Collect, filter, and normalize events from built-in and third-party sensors; **Security Event Consolidation:** Store collected events into a unified repository; **Security Incident Detection:** Analyze events from multiple sensors to detect anomalous incidents; **Security Information Management:** Unify management of sensors, events, assets, and incidents; **Security Situational Awareness:** Visualize the total security status of the monitored networks; **Federate with Other Promia Ravens:** Connect with other Promia Raven appliances for greater reach;

For more information, please contact:

PROMIA, Inc
160 Spear Street, Suite 320
San Francisco, CA 94105

415-536-1600 (Phone)
415-536-1616 (Fax)
sales@promia.com