

## CIPGuard Cyber Infrastructure Defense CIPGuard Featuring Promia's Raven™ Technology

CIPGuard incorporates Promia Raven™ technology which is based on over ten years of product development and deployment within the U.S. Department of Defense where it has won multiple awards for technological innovation. Over the past five years, Raven has become the leading information assurance product for the U.S. Department of Navy cyber infrastructure where it is now being deployed globally throughout all US Naval installations and ships.

Raven's security capabilities are unique to Nexant's NERC CIP compliance assessment and delivery services and include:

- Integrated cyber protection tools that address all CIP cyber standards and individual requirements
- Network cyber security tools accredited by the NSA (Common Criteria) and the Department of Defense (DITSCAP/DIACAP)

Raven's capabilities extend to full network security with robust, built-in features and network security options that surpass anything currently available in the power sector today. These state-of-the-art features include:

- Asset, anomaly, and attack detection using artificial intelligence
- Autonomic response behavior including intrusion prevention blocking
- Collection and correlation of logs from network and security devices, node OS, and applications
- Event analysis for incident detection and response determination
- Network layout, visualization, and asset status
- Knowledge engineering with attack ontology.

These network security features can be leveraged to provide a second line of cyber defense to augment existing systems without any disruption or need for re-architecting. Moreover, a second line of defense substantially aids in demonstrating compliance with CIP standards, and, with its built-in NERC CIP Compliance manager software, enhances your ability to support audit reviews.

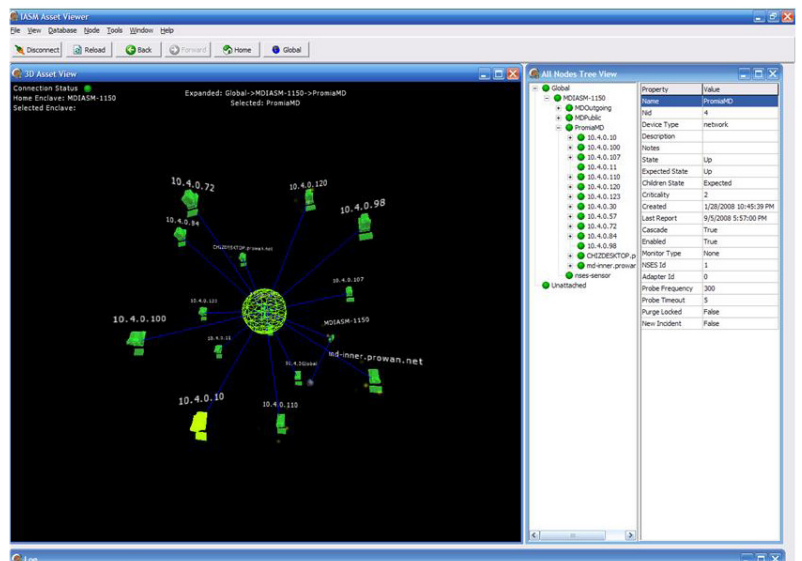
### Asset, Anomaly, and Attack Detection

The Raven technology platform capabilities include non-intrusive install and operation and features that directly support smart grid deployment, including:

- Passive asset detection—addressing and protocol information in the IP traffic is used to non-invasively detect and fingerprint assets on the network and determine the topology of assets on the network.
- Anomalous IP traffic detection with blocking—Raven uses network traffic collected during a one- to six-hour training period to develop a profile of “normal” IP traffic for the network and then monitors



Free 30-day evaluation units available



The 3-d network visualization feature in CIPGuard allows system operators to monitor and drill down on any asset in your organization, giving you real-time information

# CIPGuard

## Cyber Infrastructure Defense

### CIPGuard Featuring Promia's Raven™ Technology

subsequent network traffic to detect and generate an event for packets that deviate from the profile. The system blocks selected packets in TAP mode.

- IP packet signature matching—Raven uses the Snort™ signature matching engine to compare the content of each IP packet with known pattern rules for attacks or prohibited application behavior and generate an event when a rule is matched. Our Raven appliance support includes monthly updates of the operational rule set with the most recent rules that have been developed by the open-source Snort community and tested by Nexant for accuracy and relevance.
- Alert context capture—Raven can record 1 to 60 second “snapshots” of IP traffic both before and after a security event for later remote forensic review by skilled incident analysis personnel.

### Most Advanced Cyber-Defense Available

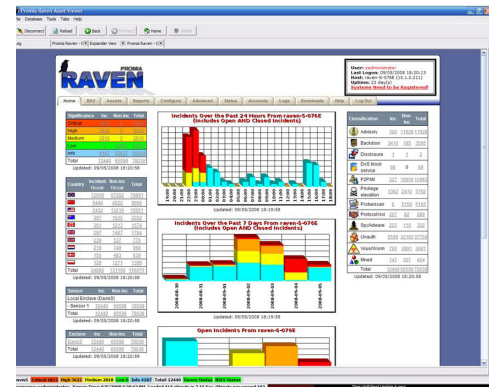
Raven cyber-defense analytics include the capability to detect multi-sensor attacks and to consider events from multiple sensor logs to detect security and operations incidents that cannot be seen from a single sensor. The algorithms are based on unique sequencing techniques, developed to support the US Department of Defense, and use a combination of artificial intelligence and statistical analysis tools to aggregate multiple related events, improving analytic speed and accuracy. The algorithms are truly unique in their ability to tag each detected incident with a natural language description of the kind of incident that is indicated by the constituent events. This feature tremendously improves the ability of operations personnel to validate and respond to detected incidents.

### Incident and Response Management

Raven tools include a standardized web interface for managing incident lifecycles, including triage, assignment, validation, remediation, and closure. Raven can be user-configured for either manual and/or automated response to detected incidents with customized pop-ups that display enterprise policy for remediation of the kind of incident detected.

### Network Status Visualization

The Raven Asset Viewer provides a powerful, three-dimensional consolidated visualization of all assets and incidents on the monitored network. This visualization is built from the model of network assets and topology generated by Raven's passive asset detection feature. This visualization allows operators to quickly see the operational and security status of the network and provides them with context for effective verification and appropriate remediation of detected incidents.



Screenshot of the Enterprise Security Management dashboard

#### Contact

**Hugh McDermott**

Senior Vice President

tel +1 415 369 1108

email hmcdermo@nexant.com

Nexant, Inc.

101 Second Street, 10th Floor

San Francisco, CA 94105 USA

tel +1 415 369 1000

fax +1 415 369 0894

[www.nexant.com](http://www.nexant.com)

