



TRIGEO UNVEILS LARGEST ACTIVE RESPONSE REPOSITORY FOR MID-MARKET ENTERPRISE NETWORK SECURITY

Company's Active Responses Enable Customers to Effortlessly Activate Network Defenses

POST FALLS, IDAHO – (August 8, 2005) – TriGeo Network Security (www.trigeo.com), the pioneer and leader of Automated Remediation through Intelligent Correlation™, today announced the availability of TriGeo Security Information Manager (SIM) v3.1 with a new Action Framework providing the industry's largest repository of active responses. Combined with over 500 preconfigured correlation rules, these active responses enable security professionals to identify security and network alert conditions, and respond with active responses that remediate attacks and enforce network policy, without complex programming.

Sophisticated correlation rules are used to detect suspicious and malicious behavior. Upon detecting a security threat, TriGeo SIM initiates a real-time response and activates the network's own defenses, based on policies the security team created in the Rule Builder or enabled from the hundreds of preconfigured rules. Some of the new response features include:

- **Remote desktop access** after business hours, terminate the offending application
- **PC showing worm behavior**, disable machine account to prevent further access to other domain resources
- **Administrative User accessing inappropriate files** (accounting, HR, etc), suspend privileges by removing them from the Administrative groups
- **User stops AV service** on their PC outside of normal maintenance window, automatically restart AV service(s)
- **Inappropriate web surfing on a PC**, send a popup message warning that further attempts will be reported to HR
- **Launch of known spyware** processes on an PC, kill the spyware processes
- **User attempting access to clearly inappropriate files**, force logoff and disable user account.

With an appliance-based solution, preconfigured correlation rules, and automated remediation capabilities, TriGeo is specifically targeting the small to medium sized enterprise. Defined as businesses ranging from 50 to 5,000 users, these businesses have unique needs that are not being addressed by SIM vendors targeting the Fortune 500.

There are several reasons why mid-sized organizations gravitate towards automating security event tasks. One reason is that smaller organizations tend to lack the staffing and infrastructure to support 24/7 security operations centers, this may affect their ability to react quickly to a security incident.

According to Amrit Williams, research director for Gartner, Inc., “Any time you can automate a manual process to achieve greater efficiencies and faster response time organizations are going to be receptive to that; especially when the organization has resource constraints.”

Michelle Dickman, CEO of TriGeo Network Security agrees. Dickman notes that mid-market organizations face significant staff and budget constraints and are implementing automation to maximize those resources. “The small to mid-sized enterprise teams welcome automation for the simple reason that they can’t provide 24/7 coverage and are already stretched thin,” said Dickman. “Our active response technology is a unique capability that sets us apart from traditional SIM players, and is fast becoming the must have requirement for success in this space.” With the release of version 3.1, TriGeo extends its lead in the market for SIM-based event correlation and automated remediation.

About TriGeo Network Security

Formed in 2001 as the pioneer and leader of Automated Remediation through Intelligent Correlation™ for securing small and medium-sized enterprise networks, TriGeo protects your entire network environment--from perimeter to endpoint—with a comprehensive, integrated solution. TriGeo is the leading real-time security information management appliance that automatically identifies, notifies and responds to suspicious behavior, policy violations, and network attacks.

TriGeo is a privately held company headquartered in Post Falls, Idaho. For more information, visit the company’s website at www.trigeo.com or call (208) 664-7000.

#