



## **CHICAGO STOCK EXCHANGE BULLISH ON TRIGEO'S REAL-TIME LOG ANALYSIS, THREAT ASSESSMENT AND REMEDIATION**

*Exchange is able to identify and respond to network security threats using policies they've created and tuned to their environment*

**POST FALLS, IDAHO** – (May 2, 2005) – TriGeo Network Security ([www.trigeo.com](http://www.trigeo.com)), the pioneer and leader of Automated Remediation through Intelligent Correlation™, today announced that the Chicago Stock Exchange bought the powerful new version 3.0 of TriGeo Security Information Manager (TriGeo SIM), a self-contained appliance that runs on a hardened version of Linux. With TriGeo, the Chicago Stock Exchange (CHX) can analyze, compare and correlate several thousands of lines of log files from more than 1,000 dissimilar devices on their network into one centralized console.

"There are a lot of products out there," said Leilani Lauger, Information Security Manager of Chicago Stock Exchange. "TriGeo's product actually did what they said it would."

A self-regulatory organization under the oversight of the U.S. Securities and Exchange Commission (SEC), CHX currently consists of approximately 200 member organizations and a staff of over 200. With nearly half of its staff employed in information technology, CHX needed to utilize state-of-the-art technology such as TriGeo's event correlation to meet the needs of investors in a very demanding global financial environment, where more than 3,500 NYSE, Amex, NASDAQ and CHX-exclusive issues are traded.

In-memory, event correlation is the brains behind both TriGeo's notification and automated remediation capabilities. Unlike data mining systems, the event analysis takes place entirely in memory. This allows CHX real-time performance even under attack scenarios when databases can be bound by insertion rates.

CHX took some of the 500 preconfigured rules that shipped with TriGeo, and cloned them into its own repository of enabled rules. CHX started using preconfigured rules for events such as accounts being disabled and attempts to access privileged accounts. CHX then built more rules that addressed things they weren't necessarily looking for including worms and Trojans, but knew could happen. Most of the rules were built as Priority Alerts

and use TriGeo's automated notification to track down IT staff when they're busy with other tasks.

TriGeo's configurable rules and policies allow users to define what events merit alert status. When those events occur, TriGeo can instantly notify and transmit security alert information to CHX through email, cell phones, pagers, and handheld devices. With TriGeo, CHX can respond to threats in real-time by invoking user-defined policies that can block an IP address, reroute traffic, and quarantine a workstation or a number of other active responses.

### **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](http://www.trigeo.com) or call (208) 664-7000.

# # #