

Tenable Expands Capability for Enterprise Class Log Management and Forensics

Tenable releases full log aggregation, compression and search capability for its Unified Security Monitoring Suite

May 20, 2009 – Columbia, MD – Tenable Network Security, Inc., the leader in Unified Security Monitoring and creator of the popular and award-winning Nessus vulnerability scanner, today announces the release of Security Center 3.4.4 and Log Correlation Engine 3.2 for general availability. With this release, Tenable now offers enterprise customers full log aggregation and search combined with sophisticated user tracking, anomaly detection and correlation in one fully integrated product offering.

Full Log Aggregation, Search and Forensic Analysis

This latest version of the Log Correlation Engine allows powerful and rapid searches of large amounts of log data gathered from routers, operating systems, security applications, firewalls and much more. Any log that is gathered can be automatically indexed, compressed and searched.

Multiple Log Correlation Engines can be used to work together in a distributed fashion for larger enterprise environments. This allows logs to be gathered and compressed in one location and for searches to be performed across an entire enterprise.

Each Log Correlation Engine retains a full copy of every log it receives, which is very important in forensic investigations. Logs from multiple sources, such as access control devices, firewalls and intrusion detection systems can be gathered and searched in one place. This simplifies the collection of evidence that indicates abuse, misuse or data compromises.

User Tracking, Anomalies and Correlation

The Log Correlation Engine has excellent features for security monitoring of network resources. These features include:

- Automated user tracking, enabling a clear method of understanding and visualizing what network and application activities are occurring in the environment
- Automated “first seen” and “statistical” profiling of any event and any log source enables analysts to identify change in near real time, and also understand changes in activity level across the network
- Event correlation to automatically identify devices that have been compromised by worms, web applications that are under attack and determined attempts to manually compromise the network.

Tenable’s Log Correlation Engine is easy to set up and contains thousands of normalization rules that are enabled “out of the box”.

“With the release of the full aggregation and search capability, Tenable now delivers a powerful event management solution with the capability to search logs in an ad hoc fashion which is in high demand by CIOs for forensic analysis of incidents on their networks,” says Ron Gula, CEO of Tenable Network Security.

About Tenable Network Security®

Tenable Network Security is the leader in Unified Security Monitoring. Tenable provides enterprise class agentless solutions for continuous monitoring of vulnerabilities, configurations, data leakage and log analysis and compromise detection. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit <http://www.tenablesecurity.com/>.

Contact Information:

Jack Huffard, Tenable Network Security
410-872-0555
media@tenablesecurity.com