Raz-Lee Security Extends SIEM Support to LEEF, CEF & Multiple Concurrent SIEMs

Nanuet, New York – April 5, 2016 - Raz-Lee Security Inc., a major vendor of security, auditing and compliance software solutions for IBM i systems, announces the availability of extended Syslog for SIEM support.

Following are some of the highlights of the extended support:

- Field-mode formats for IBM QRadar (LEEF) and HP ArcSight (CEF) are supported; each event value is stored in a separate field together with its appropriate descriptive name. Previous support for LEEF/CEF and other standards, with messages that integrate field values within a descriptive message, were preserved. It should be noted that Raz-Lee is certified by IBM as "Ready for Security Intelligence" and partnered with Q1Labs prior to their acquisition by IBM.

- As more and more companies worldwide are using multiple SIEM solutions, Raz-Lee now supports up to 3 SIEM products/servers simultaneously. For example, iSecurity can send network and system related alerts to one SIEM product/server and application-related alerts to a second SIEM server. In addition, we support Imperva SecureSphere DAM and McAfee DAM and ESM (SIEM) products.

- Each of the supported SIEM products/servers is defined by its own unique destination IP, Port, CCSID, message filtering, etc.

- LEEF/CEF field mode support sends only meaningful fields. For example, since Move and Rename objects have the same Audit Type but different sub-types, the fields sent will be those relevant to the activity to the object.

- UDP, TCP and encrypted TLS protocols are all supported.

- Advanced communications recovery features have been implemented where feasible, in the event of network problems or SIEM unavailability.

The extended Syslog support capabilities and features are a direct result of increasing customer demand for integrating IBM i (AS/400) security-related event alerts with SIEM solutions.

"Raz-Lee is excited to be able to offer the market advanced Syslog capabilities which supplement our existing partnerships, such as our DB/400 Agent for Imperva SecureSphere and our McAfee-certified DAM (database activity monitoring) and ESM (SIEM) solutions" said Shmuel Zailer, CEO at Raz-Lee Security. "The proven integration of all iSecurity solutions with products from IBM, HP, Splunk, Juniper, RSA, GFI, NTT, CA and others once again establishes Raz-Lee's position at the leading edge of IBM i technology."

About Raz-Lee Security Inc. and iSecurity

Raz-Lee Security, headquartered in Nanuet, New York, is the leading security solution provider for IBM's IBM i (AS/400) midrange computers. Drawing upon its more than 32 years of expertise in the IBM i market, the company designs, develops and markets a comprehensive suite of more than 20 advanced security software solutions, iSecurity.

Raz-Lee's iSecurity product suite is field-proven at thousands of sites, ranging from sites with more than 200 systems thru SMBs and single-LPAR P05 installations, in more than 40 countries worldwide.

For further information please contact:

Eli Spitz
Vice President, Business Development
Raz-Lee Security Inc.
Tel: 1-888-729-5334
E-mail: eli.spitz@razlee.com
www.razlee.com