iSecurity

DATASHEET

iSecurity SYSLOG to SIEM

Overview

Integration with SIEM products for forensic analysis of security-related events is an increasingly important requirement at companies worldwide; indeed, Raz-Lee's iSecurity suite has supported Syslog-to-SIEM for numerous years. The latest version of Raz-Lee's Syslog-to-SIEM support includes market-critical requests described in this data sheet.

Features

- Proven integration with all SIEM products.
- Field-mode support for the 2 major standards – LEEF (IBM QRadar) and CEF (ArcSight). These standards are supported in many other SIEM products as well.
- As an alternative to CEF and LEEF, iSecurity continues to support local structuring of the message format sent to a specific SIEM.
- Sends Syslog messages in parallel to up to 3 SIEM products.
- Transmission is supported via UDP, TCP or TLS (encrypted channel).
- Support in all iSecurity solutions enables infrastructure-related alerts and field-level application alerts on unauthorized data changes or access.
- Advanced filtering capabilities via specific severity code, part of the syslog standard, for each event/message and specifying the range of messages to send to each SIEM. This controls which messages will be sent to each SIEM.
- Advanced communications recovery features handle network problems or SIEM unavailability
- Enables sending extremely high volumes of information with virtually no performance impact.
- Syslog Self-Test facility runs on the IBM i, receiving messages locally for syslog message pre-check prior to sending to a remote syslog server.

Success Stories

Insurance Company

- Sends all application data changes to SIEM
- Sends all DB updates (more than 1000 transactions/second), with CPU overhead <1%
- Sends system journal (QAUDJRN) & network access alerts to SIEM

Mortgage Bank

- Sends all network access rejects to SIEM
- Sends important system journal (QAUDJRN) events to SIEM
- SIEM performs advanced forensic analysis of messages from all platforms
- Use iSecurity to provide audit reports to both internal and external auditors

Bank

- Sends messages to 2 SIEMs simultaneously
- Different types of information are sent to each SIEM as they are managed by different groups in the bank