iSecurity Syslog

Real Time IBM i Security Event Communication

SEA™ SOFTWARE ENGINEERING OF AMERICA

Software Engineering of America
info@seasoft.com www.seasoft.com 516.328.7000

iSecurity Syslog

iSecurity Syslog provides real-time transmission of IBM i (AS/400) security event information to enterprise SIEM solutions.

With the growing need for companies to integrate security data into Security Information Enterprise Management (SIEM) solutions to gain an enterprise level view of security as well as comply with regulatory requirements, the IBM i's role of hosting critical business applications has made the IBM i an essential part of integrating security data into an enterprise SIEM solution.

About iSecurity Syslog

iSecurity Syslog provides transmission of event information for standard IBM OS400 audit types as well as specific iSecurity Audit entry types to provide additional details beyond what QAUDJRN currently provides, including:

- Security related events involving changes to configuration, validation lists, verification functions & security runtime functions
- Authority failure, Password reset, Use of adopted authority and program integrity violations
- Object access auditing for creates, deletes, reads or changes
- Job changes, Moves or renames of objects, & Operations on spooled files
- Save or Restore operations
- Service Tools and System management activities
- Advanced Peer to Peer Network communications, System distribution or office mail or Optical volumes tasks, and Attention events
- iSecurity internal custom audit types used to generate reports over multiple IBM standard audit types

Features of iSecurity Syslog

- Encryption of Syslog Messages sent – supports UDP, TCP with Transport Level Security (TLS) encryption
- Support 3 Parallel SIEM, where Adjustable Port, Severity, Facility, Length can send in CEF (HP ArcSight and more), LEEF(IBM QRadar), User edited mode that include all audit types
- Support separate handling for each SIEM with problem detection, so that when connectivity problems are detected the process waits for recovery before sending resumes
- Support for McAfee DAM (by JSON) and Imperva SecureSphere
- Supports "Super Fast' Transfer method - "Super fast" iSecurity Syslog implementation enables sending extremely high volumes of information with virtually no performance impact.
- Customizable product configurations which aid integration with any Syslog products

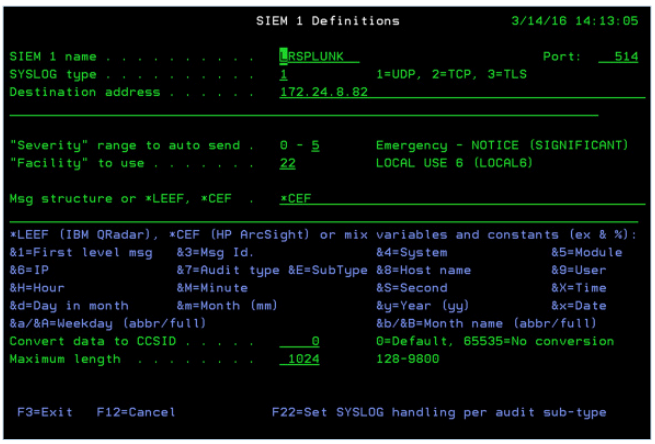

Figure 1 – iSecurity Syslog Definitions by SIEM

Integration with Leading SIEM solutions

iSecurity Syslog provides an additional layer of security to an IBM i enterprise by sending messages to SIEM solutions by integrating IBM i (AS/400) security data with the rest of the enterprises security information.

iSecurity Syslog integrates with industry leading SIEM solutions such as:

- IBM (QRadar)
- Mcafee
- RSA
- Imperva (SecureSphere)
- Splunk
- GFI
- Arcsight
- AllianceOne
- Alien Vault
- LogRhythm
- Juniper
- Manage Engine
- And More

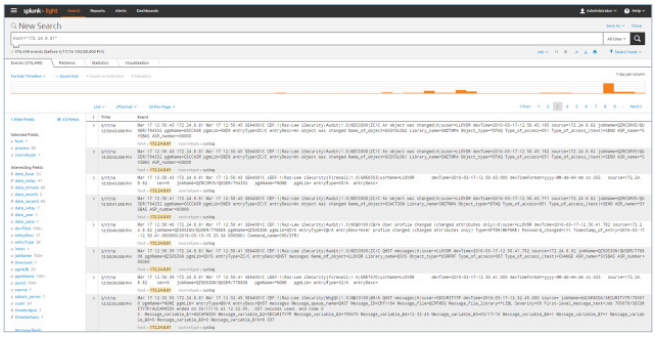

Figure 2 – iSecurity Syslog integration with Splunk showing CEF, & LEEF formats in addition to QHST

Support of Key iSecurity Solutions for transmission of Security Event Information

iSecurity Syslog provides real-time alert handling and integrates seamlessly with the following iSecurity solutions to send security event information:

- iSecurity Audit - Audit Journal Messages (QAUDJRN), QHST, and any selected Message Queues
- iSecurity Firewall - Network Security & Exit Point Activity
- iSecurity AP-Journal - Database Journal Activity
- iSecurity Authority On Demand - User Authority Changes
- iSecurity Anti-Virus - Virus Quarantine Activity

iSecurity Audit – Advanced Auditing & Compliance Integration

iSecurity Syslog's integration with iSecurity Audit allows advanced capabilities including the ability to:

- Transmit audit entry types and specific QAUDJRN journal entry types which have been processed by iSecurity Audit's real-time advanced filtering
- Transmit QHST, QSYSOPR & QCPFMSG logs with real-time action filtering
- Use Real Time alerts to send Customizable events to an enterprise SIEM

iSecurity Firewall – Exit Point Activity Integration

iSecurity Syslog integration with iSecurity Firewall provides transmission of all exit points transactions that are monitored by iSecurity Firewall and can send all transactions or a defined subset of transactions to a SIEM, including:

- Transactions from 44 plus access servers shipped with the operating system
- Transactions which are 'logged only' (both allows and rejects) remote events using iSecurity Firewall's FYI mode, which allows users to do simulate rules before going live.
- Filtered remote server transactions by severity assignment

iSecurity Authority On Demand Integration – User Authority Management Integration

iSecurity Syslog's integration with iSecurity Authority On Demand provides users with the capability to transmit authority change information logged in iSecurity Authority on Demand to SIEM solutions, including:

- Start and End of the elevated Swap or Added authority or special authority
- Reason for the elevated authority requests
- Failed elevated authority attempts

iSecurity Application Journal – Field Level Change Monitoring Integration

iSecurity Syslog's integration with iSecurity AP-Journal allows users to send field level before and after database journaled transactions as they occur, including:

- Unauthorized read access of sensitive database files residing in critical production libraries
- Real-time updates on confidential database records in various business critical applications
- Triggers on changes to sensitive database information as they occur

iSecurity Anti-Virus – System Anti-Virus Integration

iSecurity Syslog's integration with iSecurity Anti-Virus provides companies with the ability to forward the real-time virus alerts upon detection of infection, including :

- Captured and Quarantined virus information