Alliance LogAgent for IBM QRadar
Data Sheet

Log Collection and SIEM Integration for the IBM i

Meet PCI, SOX, HIPAA, GLBA and other security compliance regulations for log collection and monitoring. Alliance LogAgent collects security journal (QAUDJRN), system operator, QHST, and user security messages for distribution to IBM Security QRadar. Alliance LogAgent for IBM QRadar supports Log Event Extended Format (LEEF) messages and integrates with Alliance encryption and Internet communications solutions.

High Speed Event Management

Poor performance can consume CPU resources and slow event management, defeating your security strategy. On an entry level IBM i platform, Alliance LogAgent processed over 2,000 events per second with minimal impact on CPU.

Townsend SECURITY

Meet Compliance Regulations
Collect security system logs and transmit to the IBM Security QRadar log collection server

Formats QAUDJRN Security Journal
Format to the IBM Security QRadar Log Event Extended Format (LEEF)

Communicates Securely
Communicates with log collection servers and Security Information & Event Management (SIEM) solutions

High Performance
Event management protects CPU resources with high event processing speeds

Affordable Solution
Protects your investment in IBM i hardware and software

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360.357.9047

Log Collection

- System security journal QAUDJRN
- User entries in security journal QAUDJRN
- Operator message queue QSYSOPR
- QHST system log messages
- User application messages
- Apache, Websphere, PHP, MySQL, OpenSSH and other messages with syslog-ng
- IBM exit points
- File Integrity Monitoring events

Syslog-ng

- IBM i version for Apache, Websphere, PHP, OpenSSH, log collection

Storage Management

- Remote archival for QAUDJRN entries reduces System storage
- Use system management for QAUDJRN journal receivers

Communications

- Standard syslog UDP protocol
- Standard syslog TCP communications
- Standard syslog TLS secure communications

Log Filtering

- Filter security audit journal QAUDJRN by event type
- Filter QHST messages by privileged user
- Filter events based on effective user
- Selectively filter system values reporting
- Include/Exclude library objects
- Include/Exclude IFS directories and files
- Selectively enable QAUDJRN, QHST, QSYSOPR, and IFS syslog collection and reporting

API's

- Supports direct user application QAUDJRN entries
- Sends Log Event Extended Format (LEEF) messages
- Bindable service program for syslog message creation

Security Assessment

- Identify and report privileged users

System Requirements

- IBM i OS/400 or i5/OS V6R1 or later.

Support

- Software maintenance
- Technical support
- 24/7/365 support available
- On site installation available
- Contract services available

Contact Us

Townsend Security
www.townsendsecurity.com
800.357.1019
360.359.4400