



## Real-Time Security Events from the System i

### Monitor Your Most Critical Data

IBM® Power Systems™ (System i®, AS/400®) servers run some of the most critical business applications in your organization. PowerTech Interact allows you to monitor, capture, and send security-related events from these systems directly to your enterprise security monitor.

### Simple Explanations

Interact takes raw security event data from the server and converts it into a meaningful format for security operations staff. Complex audit journal details are simplified into plain English statements such as:

*"An invalid password was entered for user profile TOM"*  
*"System Value QSECURITY was changed from 40 to 30"*

### Filter Entries

You don't need to flood the network and fill up your Security Information and Event Management (SIEM) solution with every journal entry. Save disk space and bandwidth by selecting or omitting events based on key characteristics:

- Event Type
- User ID
- IP Address
- Time and Day of Week

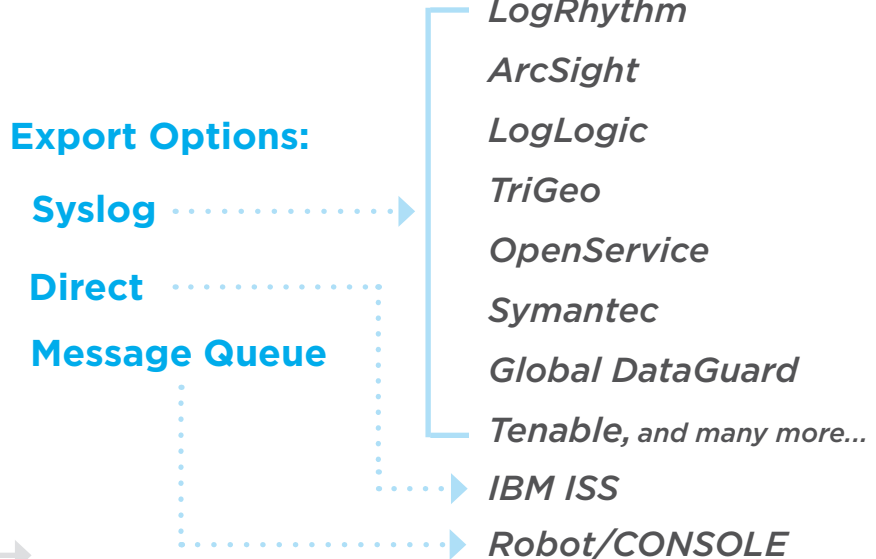
### Console Views

Your existing SIEM consoles, or shareware, can read and interpret Interact's syslog output. And, Interact writes directly to IBM ISS Site Protector format.

### Over 500 Event Types

- Security Audit Journal**  
(QAUDJRN)
- Critical OS Messages**  
(QSYSMSG or QSYSOPR)
- PowerTech Network Security Exit Programs**  
(FTP, ODBC, Remote Command)
- PowerTech Authority Broker**  
(Privileged User Tracking)

### Security Information and Event Management



## “Review logs for all system components daily.”

- Requirement 10
- Payment Card Industry Data Security Standard

### Comprehensive Coverage

Monitor over 500 different events from a variety of sources.

### Audit Journal Events

Interact captures audit journal events from the IBM security audit journal, QAUDJRN. Some of the common event types are:

- Authority Failures and Changes (AF, RA)
- Change to Authorization list (CA)
- Object Changes, Reads, Creates, Deletes (CO, ZR, ZC, DO, OM, OR, OW)
- User Profile Changes (CP)
- User and Password Login Failures (PW)
- System Value Changes (SV)
- Intrusion Detection (IM)
- Service Tools Used (ST, DS)
- Commands (CD)
- Job Start, Stop, Change (JS)

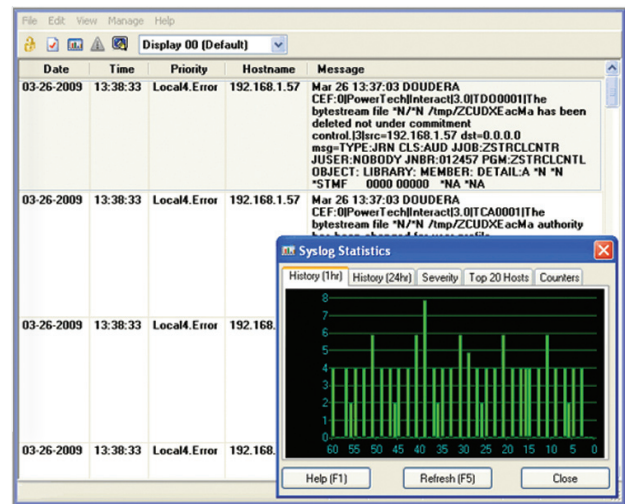
### Network Transactions

Monitor network access events logged by PowerTech Network Security exit programs:

- 33 remote-access servers, including FTP, ODBC, Remote Command
- 190+ functions
- Accepted and rejected transactions

### About the PowerTech Group, Inc.

Because Power Systems servers host sensitive corporate data, it is critical that you practice proactive compliance security. As an IBM Advanced Business Partner with over 1000 customers worldwide, PowerTech understands corporate vulnerability and the risks associated with data privacy and access control.



IBM System i events in a Security Information and Event Management (SIEM) display.

### Critical Operating System Messages

Interact includes 66 distinct critical OS messages, such as:

- Disabled Profiles
- Disk Space Limit Exceeded
- Audit Journal Changes

### Discover Interact Today

With Interact, you enjoy all the benefits of centralized, real-time notification of System i security events directly on your Enterprise security console.

To learn more, visit [www.powertech.com](http://www.powertech.com) to find white papers, case studies, and product demonstrations, or call 800-915-7700 (USA) or 253-872-7788 to speak to a security solutions specialist.

