helpsystems

DATASHEET *(Cybersecurity)*

Powertech SIEM Agent for IBM i

Monitor Your Most Critical Data

The IBM i OS runs some of the most critical business applications in your organization. Powertech SIEM Agent for IBM i allows you to monitor, capture, and send security-related events from IBM i directly to your enterprise security monitor.

Simple Explanations

Powertech SIEM Agent takes raw security event data from IBM i 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 JOHN"

"System Value QSECURITY was changed from 40 to 30"

PRODUCT SUMMARY

KEY FEATURES

- Security event monitoring
- Real-time notifications
- Easy-to-understand explanations
- Event filtering
- SIEM integration
- Multiple export options

SYSTEM REQUIREMENTS

IBM i 7.1 or higher

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

Virtually every SIEM console can read and interpret Powertech SIEM Agent's syslog output. Powertech SIEM Agent also writes directly to IBM ISS Site Protector and has received HP ArcSight Common Event Format (CEF) certification.

Comprehensive Coverage

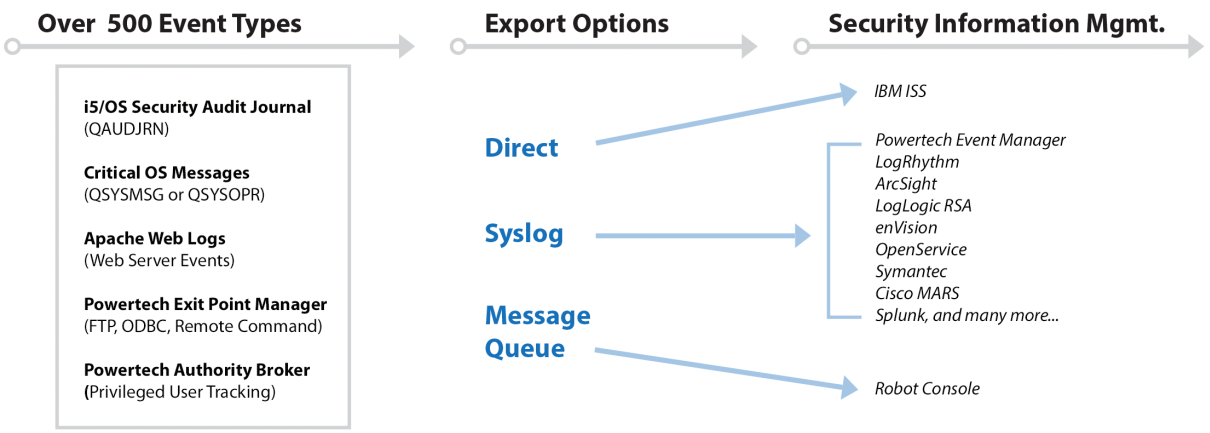
Monitor over 500 different events from a variety of sources.

Audit Journal Events

Powertech SIEM Agent captures audit journal events from the IBM i 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)

Virtually every SIEM console (including HP ArcSight) can read and interpret Powertech SIEM Agent's syslog output for enterprise-wide visibility.



Network Transactions

Monitor network security events logged by Powertech Exit Point Manager:

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

Apache Web Logs

Powertech SIEM Agent captures Apache web server events and forwards them, making it easier to integrate with your SIEM solution.

Privileged Users

Keep tabs on privileged users with profile swap activity logged by Powertech Authority Broker:

- When a profile swap starts and ends
- Reason for the swap
- Firecall swaps
- Invalid swap attempts

Critical Operating System Messages

Powertech SIEM Agent includes 66 distinct critical OS messages, including:

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

Powertech SIEM Agent provides real-time notification from IBM i. Don't use an inadequate solution that requires a batch file transfer, or worse, allow events to occur undetected.

Let's Get Started

To find out what Powertech SIEM Agent can do for you, request a demo We'll review your current setup and see how HelpSystems products can help you achieve your security and compliance goals.

LOUPREY INTERNATIONAL

(55) 5543 6515
marketing@louprey.com
www.louprey.com
Kansas #7 Piso 2, Col. Nápoles, C.P. 03810,
Benito Juárez, Ciudad de Mexico