DATASHEET

PowerTech your security expert

PowerTech Interact

Real-Time Security Events from IBM i

Monitor Your Most Critical Data
The IBM i OS runs some of the most critical business applications in your organization. PowerTech Interact™ allows you to monitor, capture, and send security-related events from IBM i directly to your enterprise security monitor.

Simple Explanations
Interact 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"

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 Interact's syslog output. Interact also writes directly to IBM ISS Site Protector and has received HP ArcSight Common Event Format (CEF) certification.

Over 500 Event Types

i5/OS Security Audit Journal
(QAUDJRN)

Critical OS Messages
(QSYSMSG or QSYSOPR)

Apache Web Logs
(Web Server Events)

PowerTech Network Exit Programs
(FTP, ODBC, Remote Command)

PowerTech Authority Broker
(Privileged User Tracking)

Export Options

Direct

Syslog

Message Queue

Security Information Mgmt.

IBM ISS

LogRhythm
ArcSight
LogLogic
RSA enVision
OpenService
Symantec
Cisco MARS
Splunk, and many more...

Robot/CONSOLE
Bytware Messenger

The PowerTech Group, Inc.
www.powertech.com • info@powertech.com

TEL USA: 253-872-7788
TOLL FREE: +1 800-915-7700
TEL UK: +44 (0)870 1203148

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

ArcSight CEF Certified 2013

Comprehensive Coverage
Monitor over 500 different events from a variety of sources.

Audit Journal Events

Interact 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)

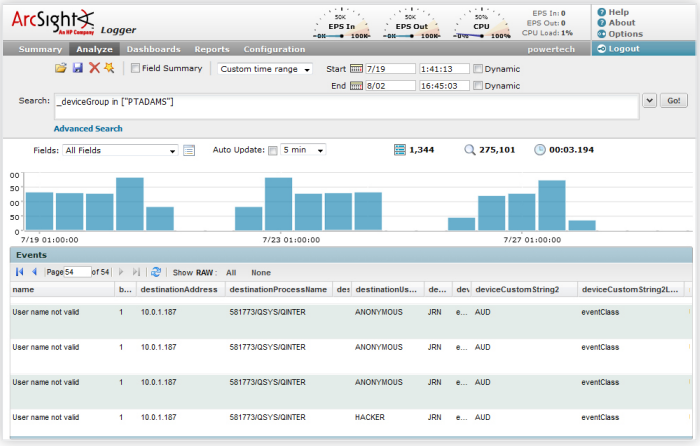
Network Transactions

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

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

Apache Web Logs

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



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

Privileged Users

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

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

Critical Operating System Messages

Interact includes 66 distinct critical OS messages, including:

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

Interact 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.

About the PowerTech Group, Inc.
Because Power Systems™ servers are used to host particularly sensitive corporate data, it is imperative 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.

To learn more, visit 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.

IBM Business Partner