PowerTech
your security expert

WHITE PAPER

Integrating IBM i Security Events into Your SIEM

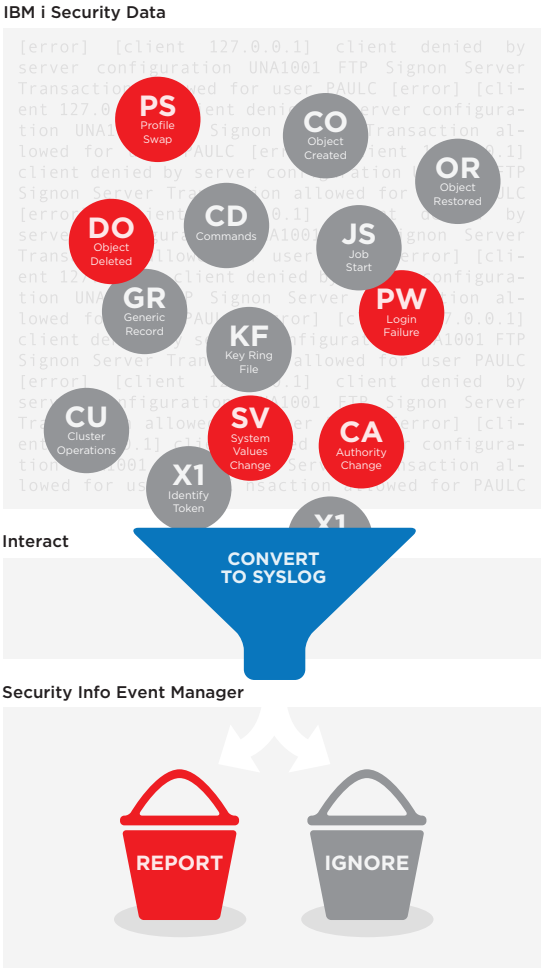
Power Systems servers run some of the most business-critical applications in enterprises around the world. You would think that the server housing the most confidential and critical data would get the most security attention, right? Unfortunately, that is rarely the case. In reality, IBM i security is often poorly configured or even ignored.

While many companies use Security Information and Event Management (SIEM) solutions to comply with regulations, these SIEM solutions offer no coverage or, at best, only weak coverage for Power Systems servers running IBM i (AS/400, iSeries, System i). This paper discusses the technical issues relevant to logging IBM i security data and offers a solution for real-time awareness of security events and integration with SIEM solutions.

IBM i – The Home of Business-Critical Data

In the summer of 2013, IBM celebrated the 25th anniversary of the launch of the AS/400 midrange server and its corresponding operating system, OS/400. Through years of successful growth in the 1990s, this reliable platform has become an integral part of IT operations for organizations worldwide.

It is estimated that there are over 350,000 systems in active use running these types of mission-critical



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) 870 120 3148

applications such as enterprise resource planning, retail, hospitality, and core banking.

Although IBM does not sell large quantities of the system into new accounts now, it continues to maintain a passionate and loyal user base. Users appreciate the simplicity of the object-based architecture, unique features like single-level storage, and the fact that the DB2 database is integrated into the operating system.

Today, IBM markets the IBM i OS as part of the Power Systems platform alongside AIX and UNIX. IBM i incorporates TCP/IP networking technology and there is even a file system to store UNIX and Windows files.

Regulations – Driving the Need for Security Logging

The business applications running on IBM i house critical data, such as credit card data, social security numbers, bank account information, and customer and patient records in the integrated DB2 database. In recent years, Sarbanes-Oxley, HIPAA, PCI, and GLBA regulations have placed increased emphasis on the need to adequately control and secure such information. Along with preventive measures, organizations around the world are implementing a tighter set of detective controls over the configuration and use of their business applications and servers. Many companies have adopted frameworks such as ISO 27002 and COBIT to guide the definition and implementation of their security policies. New requirements for SOX, HIPAA, PCI, and many other regulations require close monitoring and analysis of activity logs on critical systems.

The Payment Card Industry Data Security Standard (PCI DSS) has defined some of the most specific requirements of any regulation—logs must be reviewed daily and a minimum of three months' logs must be immediately available for analysis. Recent regulations like the Nevada Gaming Commission Minimum Internal Control Standards (MICS) have followed the lead of the credit card industry and imposed similarly stringent requirements. *See the Appendix for specific text from some of the regulations and standards that drive the need for more logging and auditing of information.*

Despite the importance of the data it stores, security is often poorly defined and configured on IBM i. A recent study showed that, on average IBM i servers had over 65 users with root-level authority[1]. The typical system has 79 users with default passwords that are the same as the user name.

Today the emphasis of general security spending has shifted away from perimeter security (firewalls, anti-virus, and intrusion detection) to compliance initiatives and guarding against the insider threat from employees.

Auditors now demand that IBM i logs and event data receive the same level of monitoring and attention as other platforms. IT executives and security management expect that log data and events from the platform running their most critical business applications should receive the same level of attention as their firewalls, switches, Windows, and UNIX databases.

Security Information and Event Management

Driven by the wave of regulations, a new class of security solution provider has emerged called Security Information and Event Management. Gartner's Magic Quadrant for this category tracks over 16 vendors, including: HP ArcSight, McAfee, Splunk, EMC RSA, SolarWinds, Symantec, Q1 Labs, and Tibco LogLogic.

SIEM solutions provide reporting and analysis of data from host systems, applications, and security devices and correlate and aggregate data from many different sources, providing the reports that are required for internal audits and compliance. These SIEM solutions also provide event escalation and alerting functions that support the incident management and response needs of the IT security organization. Correlation engines analyze network data in real time and look for patterns and trends—for both internal and external threats. Solutions that were originally developed as a way to manage the vast quantity of data from intrusion detection systems are now being used to monitor identity and access logs for compliance purposes. Recent trends in the SIEM market have seen a new focus on logs provided by applications.

1 The PowerTech Group, *2013 State of IBM i Security Study*, 9-11.

Syslog – Data Logging Standard

SIEM tools often use a computer data logging standard called syslog to integrate security event data from multiple sources into a central repository. Syslog was developed in the 1980s and is now supported by a wide variety of devices across multiple platforms, including Power Systems servers.

Syslog exchanges data in TCP/IP networks using a simple protocol. The syslog sender sends a small text message (less than 1024 bytes) to the "syslog daemon" or "syslog server". Messages are labeled with a facility code (indicates the type of program logging the message) and assigned a severity (emergency, alert, critical, error, warning, notice, info, debug). Almost all SIEM solutions can accept a feed from a syslog server.

IBM i Log Files and Auditing

Enterprises are now expecting that SIEM solutions also include data from IBM i, but this has proven problematic. One of the very powerful features of the operating system is the ability to log and record pretty much everything that happens on the system to a secure audit journal. This journal, QAUDJRN, is tamperproof—once an event is logged to the journal, it cannot be changed.

Many people do not use the logging capability because they are unsure how to configure it to selectively gather events of importance (i.e., event types, objects, and user profiles). Additionally, the audit journal can consume enormous quantities of disk space (50 GB per day is common) and the data logged is difficult to read and interpret.

There are over 70 different types of security events and transactions that the OS can record to the journal. Many vendors, including PowerTech, have also leveraged the power and integrity of the audit journal to log and record their own transactions. Some of the relevant activity that can be gleaned from QAUDJRN includes:

- Invalid login (sign-on) attempts
- Command usage by specific users
- Creation, movement, restoration, and deletion of objects (including database files)
- Changes to system values and user profiles
- Authority failures
- FTP and ODBC network transaction details
- Profile swapping activity

There are three simple steps to set up IBM i security auditing, and the operating system provides for granular controls by object and user profile:

1. Security Auditing is configured using the Change Security Auditing (CHGSECAUD) command. The level of auditing can be configured using the QAUDLVL system value. Table 1 provides a recommended set of settings.
2. Specify sensitive and critical files to be audited using the Change Object Auditing (CHGOBJAUD) command.
3. Specify auditing for powerful or privileged users using the Change User Auditing (CHGUSRAUD) command.

The PowerTech white paper "Configuring Auditing in the Real World" provides a much more detailed guide for configuring and adjusting audit controls on IBM i, along with explaining appropriate settings for these parameters. Table 1 on the next page indicates some of the QAUDLVL controls that are used to turn on common event types.

TABLE 1: RECOMMENDED AUDIT LEVEL SETTINGS (QAUDLVL)

*AUTFAIL	Records failed sign-on attempts and unauthorized attempts to access files and other objects.
*SECURITY	Records many security-sensitive operations such as changing a system value, resetting the QSECOFR DST password, and changing object authority and ownership.
*SERVICE	Records the use of System Service Tools (STRSST) and Dedicated Service Tools (DST).
*SYSMGT	Logs changes to certain system management areas.
*SAVRST	Logs restore actions to security sensitive objects.
*DELETE	Records the deletion of any object.
*OBJMGT	Records object move and rename operations (you need this only on a production box).
*PGMFAIL	Records programs running restricted MI instructions or accessing internal OS/400 structures through unsupported interfaces.

Figure 2 shows an example of an event as it appears when the journal is viewed directly using the native IBM i commands. Sometimes the event contains binary data that requires an API to read the full details. Even if you can figure out the right parameters in the DSPJRN command to view events of interest, it's quite difficult to read and understand the events that are displayed. Auditing to QAUDJRN isn't useful without a product that captures the events into an interface for subsequent review and reporting. Ideally these events would be included in the same SIEM solution used enterprise wide.

FIGURE 2: AN AUDIT TRAIL ENTRY VIEWED DIRECTLY IN IBM i

Network Access Monitoring

Along with events that are written natively by the operating system, vendors can also log important security events. Over the years, IBM has extended the power of IBM i by adding tools that allow data to be accessed from other platforms, including PCs. Well-known services such as FTP, ODBC, JDBC, and DDM are active and ready to serve up data across the network as soon as the machine is powered on.

The operating system does not provide a native log of such network activity, but IBM has provided a means to mitigate this exposure by creating 'exit points' at the network services. An 'exit program' that is attached (registered) to the exit point can be used to monitor and log access through the network services. IBM i exit programs can also be configured with access control rules that limit access through network services based on user names and IP addresses. A well-written exit program will log and record network activity to secure, and write-once, tamperproof journals like QAUDJRN.

Too Much of a Good Thing

IBM i can produce vast amounts of audit logs—logs that are often of little or no use if the system has not been properly configured. One production system alone can generate 10,000 events per second when object-level auditing is fully configured. Often IBM i system needs for object-level auditing are driven by the high-availability software provider and not just security and compliance considerations.

Some SIEM vendors have provided a basic level of support for IBM i in their products by providing agents. However, the solutions provided by SIEM vendors have limitations because their development teams have limited experience programming for IBM i. The SIEM vendors often don't understand the context of the events, and they don't know how to map them into their own solutions. In many cases, the SIEM vendor just converts the audit journal to a flat file and copies it over to a Windows or Linux server. This type of solution can have a huge impact on bandwidth. Additionally, solutions provided by SIEM vendors pose another serious limitation—real-time awareness of security events, as they happen, is not provided.

What to Look for in a Solution

Any agent that provides monitoring of security events as they happen on the system needs to have the following characteristics:

- Interpretation of events—translate the IBM i-specific jargon into actionable statements that IT security staff can understand.
- Documentation that explains the impact and meaning of each event.
- Filtering of events so that everything sent to the journal is not sent beyond the platform to a central logging solution. Often object-level auditing needs to be configured to support the needs of high-availability software, and events are recorded that are not relevant for security and compliance purposes.
- Filtering by day, time, IP address, user profile, and event type. Before any events are forwarded to a SIEM solution, there should be a more granular level of filtering than provided by the operating system's audit controls.
- Logging of network activity (FTP, ODBC, remote command) by exit programs.
- Integration with leading SIEM solutions so that events are also mapped and normalized to the schema used by the SIEM vendor.
- Support for logs beyond QAUDJRN; critical CPF messages from the operating system and logs from Apache web server.
- When putting software on any production IBM i system, you need to be confident that it will work on a mission-critical production system—companies want a solution that has been programmed by someone with years of experience on the platform.
- Dedicated support from a technical team with mastery of IBM i issues and implementation support from engineers that understand the platform.
- A future roadmap that shows continued investment in the product.

PowerTech Interact

PowerTech Interact™ meets all of the above requirements. The programmers that developed Interact each have over twenty years experience on Power Systems. The engineers that support the product each have over ten years experience.

Interact takes only a couple configuration steps to point to the syslog server of your choice. Several SIEM vendors have taken the syslog output from Interact and mapped it into the schema in their solution. Retailers and financial institutions are using Interact

today to meet the onerous requirements of the PCI standard. Interact monitors over 500 different events, including audit journal events, operating system messages, and Apache Web Logs.

PowerTech Network Security™ provides exit program access control and logging. When it is installed, Interact can also gather and send transactions that are logged by Network Security.

PowerTech Authority Broker™ helps you keep tabs on privileged users with profile swaps, firecall, and screen captures. When used with Interact, privileged user activity such as invalid swap attempts or when a swap starts or ends, can be gathered and sent to your SIEM solution for real-time monitoring.

Download the Interact Datasheet for more information or contact a PowerTech security advisor at +1 800-915-7700 to schedule a demo and see firsthand how Interact can solve your real-time security event monitoring needs.

About PowerTech

PowerTech, a division of Help/Systems, is the leading expert in automated security solutions for IBM Power Systems servers, helping users manage today's compliance regulations and data privacy threats.

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.

- PowerTech is a member of the PCI Security Standards Council, a global open standards body providing guidance to the Payment Card Industry Data Security Standard (PCI DSS).
- PowerTech publishes many educational white papers, including the annual State of IBM i Security Study. First published in 2004, assessments of over 1700 systems have been included to date.
- PowerTech publishes an Open Source Security Policy for IBM i as a part of its mission to promote awareness of common security challenges and ensure the integrity and confidentiality of IBM i data.
- PowerTech is authorized to issue continuing professional education (CPE) credits for IBM i security education by the National Association of State Boards of Accountancy, Inc. (NASBA).

Further Resources

- *Security Auditing in the Real World*, PowerTech white paper
- PCI Compliance for IBM i, PowerTech white paper

Appendix: Relevant Regulations and Guidance

Payment Card Industry Data Security Standard

Version 2.0—October 2010
PCI Standards Council (of which PowerTech is a member)

Requirement 10: Track and monitor all access to network resources and cardholder data.	Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.
10.6 Review logs for all system components at least daily.	Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6.
10.7 Retain audit trail history.	For at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from a backup).

COBIT 5, the Control Objectives for Information and Related Technology

Version 5 — April 2012

DSS05.04 Manage user identity and logical access.	Ensure that all users have information access rights in accordance with their business requirements, and coordinate with business units that manage their own access rights within business processes.
DSS05.07 Monitor the infrastructure for security-related events.	Using intrusion detection tools, monitor the infrastructure for unauthorized access and ensure that any events are integrated with general event monitoring and incident management.
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.	Manage the business roles, responsibilities, levels of authority, and segregation of duties needed to support the business process objectives. Authorize access to any information assets related to business information processes, including those under the custody of the business, IT, and third parties. This ensures that the business knows where the data is and who is handling data on its behalf.

(continued on the next page)

COBIT 5, the Control Objectives for Information and Related Technology (cont.)

Version 5 — April 2012

DSS01.03 Monitor IT infrastructure.	Monitor the IT infrastructure and related events. Store sufficient chronological information in operations logs to enable the reconstruction, review, and examination of the time sequences of operations and the other activities surrounding or supporting operations.
APO13.03 Monitor and review the ISMS.	Maintain and regularly communicate the need for, and benefits of, continuous information security improvement. Collect and analyze data about the ISMS, and improve the effectiveness of the ISMS. Correct non-conformities to prevent recurrence. Promote a culture of security and continual improvement.

ISO/IEC 27002:2005 IT Security

ISO27002 is an international security standard that forms the basis of the ISO27001 certification. The standard consists of a series of controls defining best practices for IT security. Unlike more general frameworks, the ISO standard is specific to only security of information technology. Some of the specific controls related to auditing and reporting of logs are listed below:

10.10.1 Audit Logging	Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations.
10.10.2 Monitoring System Use	Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.
10.10.3 Protection of Log Information	Logging facilities and log information should be protected against tampering and unauthorized access.
10.10.4 Administrator and Operator Logs	System administrator and system operator activities should be logged.
10.10.5 Fault Logging	Faults should be logged, analyzed, and appropriate action taken.
11.2.4 Review of User Access Rights	Management should review users' access rights at regular intervals using a formal process.
15.3.2 Protection of Information Systems Audit Tools	Access to information systems audit tools should be protected to prevent any possible misuse or compromise.

Other

NIST 800-53	Recommended security controls for US federal government information systems.
ITIL v3	Service Operations - Access Management and Event Management | Service Design – IT Security Management