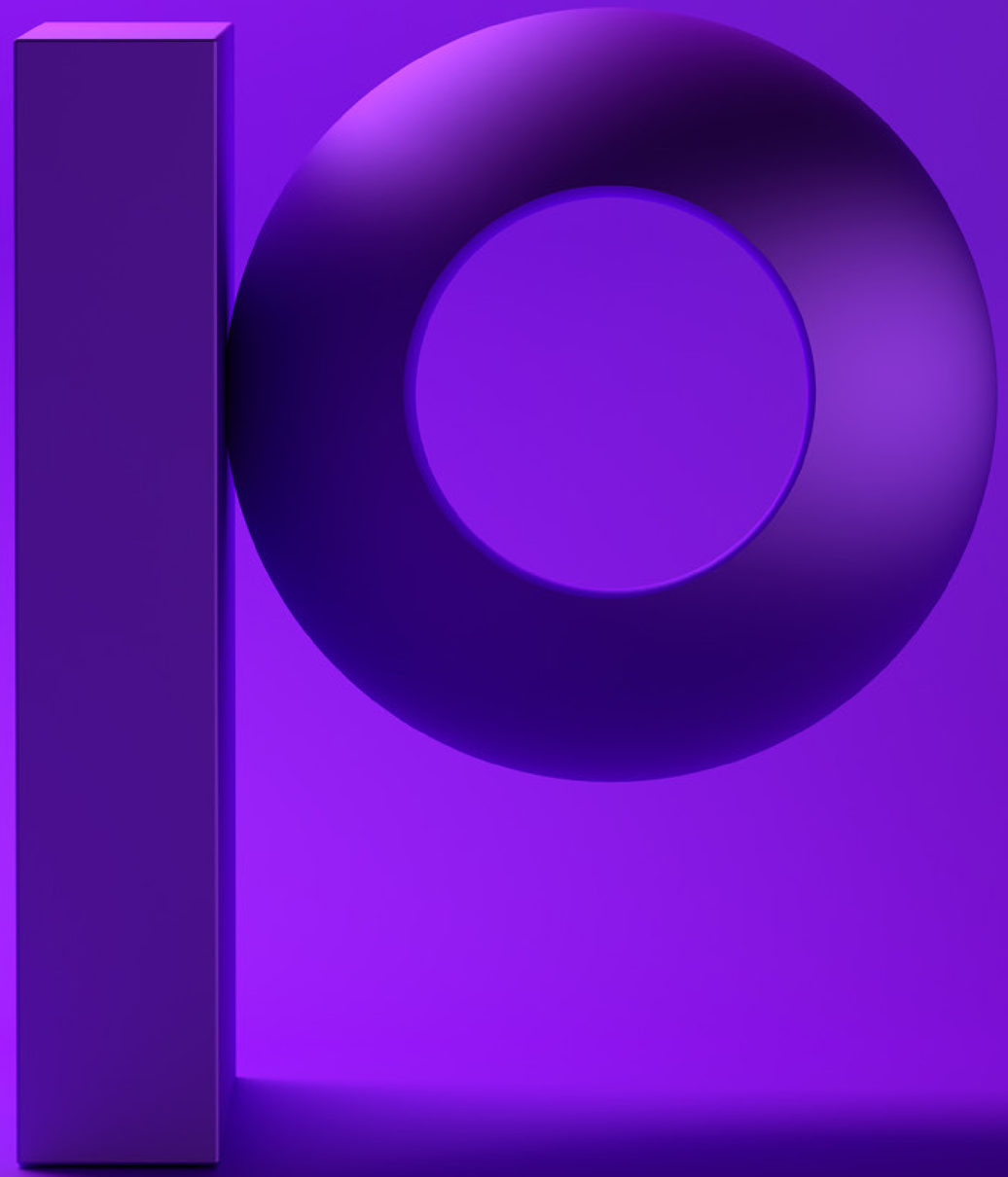
precisely

Expanding Splunk to Monitor & Analyze IBM i Security Data



Introduction

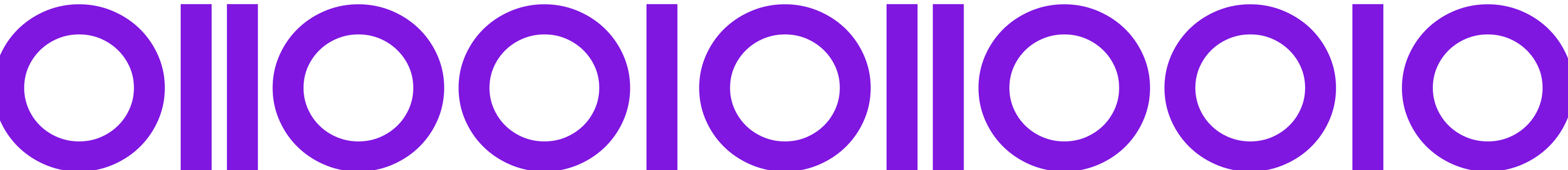
IBM i systems in large enterprises process massive volumes of critical and sensitive information every day. These systems are typically handling transaction-heavy, mission-critical workloads. In the past, they operated in relative isolation, but today most are connected to a network or the Internet, making them vulnerable to cybersecurity threats and incidents.

Sensitive data has become such a valuable commodity that not only are external threats increasing in form and fury, but internal threats are increasing as well. Even innocent mistakes can put the organization at risk. To protect data and the business in the modern landscape, IT administrators must be able to determine what's normal activity and what's suspicious. Once identified, they need the tools to react quickly to suspicious activity.

Security Information and Event Management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources.

The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources. SIEM solutions help administrators identify abnormal activity or threats by aggregating data from various sources, identifying deviations, and sending alerts or stopping operations when activity is deemed suspicious.

Many organizations are using Splunk as their enterprise-wide security nerve center. It gives teams the insight to quickly detect and respond to internal and external attacks, simplifying threat management and minimizing risk. Splunk helps teams gain organization-wide visibility and security intelligence for continuous monitoring, incident response, and provides a window into business risks. However, Splunk doesn't offer native integration with IBM i environments, so this important system can be left out — causing a significant blind spot. This eBook will explore the importance of including IBM i data into Splunk for enterprise-wide visibility, and how to do it.



How IBM i Security Data is Used in Splunk

While fairly uncommon a few years ago, technologies such as Splunk are becoming integral components in the security strategies for large, dispersed organizations. For one thing, increasingly complex compliance requirements such as PCI-DSS, FFIEC, HIPAA, SOX, and various IRS regulations, among many others, require stringent IT protection and accountability measures.

The other factor in the rise of Splunk implementations for security is the massive costs and risks of a data breach or security incident. Just one event can cost an organization hundreds of thousands of dollars in remediation costs, legal fees, fines, lost revenue, and brand damage.

Splunk helps organizations identify and remediate security issues, quicken security analysis and response times, and also automate compliance reporting through better visibility of:

- Weak passwords, passwords with no expiration, wrong or inappropriate elevated authorizes
- Weak access controls and security for critical databases, datasets, files and resources
- Network intrusions
- Data exposures to viruses or other threats
- User neglect of basic security protocols

Splunk can also correlate security data and events from various platforms, including:

- Log collection
- Log analysis
- Event correlation
- Log forensics
- IT compliance
- Application log monitoring
- Object access auditing
- Real-time alerts
- User activity monitoring
- Dashboards
- Reporting
- File integrity monitoring
- System & device log monitoring
- Log retention

Critical Information Buried in IBM i Logs

To sort out what activity is normal and what needs attention, administrators must be able to collect, manage, and analyze security information and security events from their IBM i systems. Without this ability (and visibility), data breaches are typically not found for days, weeks, or months. By the time it's discovered, the damage has been done. The organization must also be able to quickly generate accurate, readable reports for audits or risk fines or other noncompliance repercussions.

Specifically, IT administrators need to be able to access IBM i logs that contain information about a variety of dynamic elements, including:

- Changes to system objects (system values, profiles, creation or deletion of users, and authorization lists)
- Sign in and access attempts
- Any action involving sensitive data
- Access to critical databases
- Authentication failures
- Changes to passwords and access rights
- Data transmission and movement
- Powerful user activity, including the commands issued

While IBM i can be configured to log these elements and other valuable information about activity on the system, manually accessing and sorting it is prohibitively time-consuming. Accessing, sorting, making sense of it, and reporting on it for audit or security purposes is nearly impossible. To even attempt it requires time and expertise that most IT organizations' budgets and time – already stretched to the breaking points – can't support.

IBM i Log Sources

With the right tool to aggregate and query data, IBM i log sources can provide timely insights into the security of your data and systems. These sources, including journals and message queues recorded by the IBM i OS, create a comprehensive audit trail of changes. These critical log sources can be leveraged to monitor for security and compliance deviations, as well as to feed IBM i log data to enterprise security solutions that do not natively have visibility into the platform. It's important to note that by default you only have access to the history and system operations logs; you must configure logging for other log sources.

System Audit Journal — QAUDJRN

The System Audit Journal (QAUDJRN) contains information related to events occurring on the IBM i system that impact security and can be used to log user and application activity. This includes information such as changes to system values, object authorities, profiles, authorization lists, object access attempts, and more.

The audit journal is read-only and cannot be overwritten, making it a perfect container to store system security information. However, the OS logs over 90 unique types of audit entries. It's challenging to write a custom program to pull significant events from the System Audit Journal, and nearly impossible to review audit data manually.

Operator Messages – QSYSOPR Message Queue

Operator messages are alerts that inform the operator about a condition that needs attention or about changes to the environment.

System and Application Messages – QSYSMSG Message Queue

QSYSMSG is an optional message queue that gives alerts about high priority system events. It should be created and monitored continuously.

SQHST History Log

The QHST History Log is a message queue and a number of physical files that contain a list of messages that reflect certain events occurring on IBM i.

Again, making sense of the data written to many of these sources is nearly impossible. To stay compliant and monitor the security of IBM i systems, enterprises need a way to make sense of important events and quickly identify critical conditions without significant effort – or a major programming project.

Eliminating Blind Spots with Ironstream and Splunk

Splunk is designed to help assess security, vulnerabilities, and events from all the systems in an IT environment and compile it into a holistic view of security for the entire organization. By having a centralized, single system of record for security information, you can have improved security processes, and create an audit trail for reporting and compliance.

However, Splunk does not natively integrate with the IBM i platform. But Precisely Ironstream does. Ironstream makes it simple to collect, transform and securely stream IBM i security, compliance and operational log data into Splunk without specialized IBM i expertise. Ironstream seamlessly feeds IBM i security data into Splunk, ensuring that critical security data for the entire IT landscape is available in a single tool. And then Splunk can do what it does best — turning mountains of incomprehensible data into visual insights that can be used for compliance auditing, reporting, analytics, and security monitoring.

Together, Ironstream and Splunk can help you achieve satisfactory security and compliance audits, and provide security event tracking, real-time monitoring of security events, automated reporting, and complete visibility into the health and security of all systems in the enterprise.

To learn more, visit www.precisely.com/integrate

precisely

Precisely is a global leader in data integrity, providing accuracy and consistency in data for 12,000 customers in more than 100 countries, including 90 percent of the Fortune 100. Precisely enables companies to integrate, verify, locate, and enrich their data to power better business decisions. To learn more, visit www.precisely.com.

www.precisely.com