Solution Overview:

Data Provider

for IBM i, using Enforcive™/ Enterprise Security

Enforcive™/ Data Provider for IBM i is the most efficient and flexible way to collect important security events from the IBM i and provide them to an external consolidated log monitoring system. It is a comprehensive 'filter based' tool to identify a subset of the known security events and efficiently export them to the tool of your choice.

The Data Provider's management console is a GUI-based module that has been fully integrated into the Enterprise Security product, simplifying administration by using a familiar and intuitive interface.

Features:

Breadth of Data Sources. Users of the Enforcive/Enterprise Security solution already benefit from the wide variety of security and system events that are available for analysis. Enforcive/Data Provider for IBM i can collect and distribute the following data sources:

Application Audit: Connections between the IBM i and other platforms through IBM exit points and monitoring of any system or custom command.

File Audit: Information about file accesses, including before and after images of critical files.

View Data: For the most sensitive files, events can be generated from actual views and reads at databases field level.

SQL Statement Audit: Internal SQL events on the systems, including interactive SQL processes, QSHELL database functions, embedded in SQL in high level languages and queries.

System Audit: The IBM Audit journal can be analyzed for critical events.

History Log: Selected security related events from the QHST files.

Message Queue: Specific message queues can be monitored for relevant messages.

Collection Criteria. Each of the Data Sources can be analyzed using unique collection criteria. For example, with extraction of events from the IBM Audit Journal you can specify to select or omit specific groups of users, choose which of the IBM audit journal types are relevant to your extraction and even which groups of objects the events should relate to. Similarly with Application Audit the administrator can choose user departments, which exit points events are to be collected, and whether only rejections should be extracted.

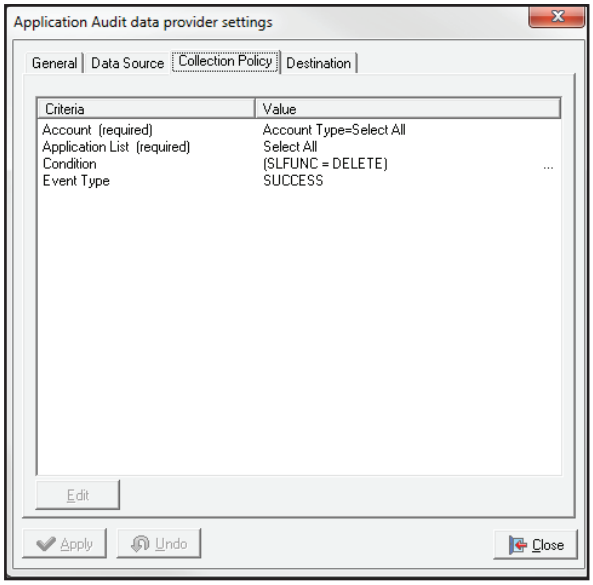

Figure 1: Selecting criteria to collect from Application Audit data

For further subsetting of the data, a Query Wizard is available to define the extraction, such as events relating to libraries beginning with Q*, or generated by a specific group of jobs.

Tailored for SIEM. The administrator can choose where to send the extracted events. Events from each data source can be sent to any Syslog server for analysis. You just need to specify the IP and port and the Data Provider will send the events in the format of your choosing. You can send events using Data Provider to many market leading log monitoring tools. For example, specific processing is available for RSA enVision and Netforensics formats. Events can also be sent to the Enforcive/Cross Platform Audit, an Enforcive product for log management, which based on Enforcive's extensive experience in the IBM i (AS400) security field, is optimized for consolidating and correlating events from multiple IBM i servers.

Data collection on your terms. In addition to the collection criteria you define for each data source, the administrator chooses whether the events need to be extracted in real time, or whether the processing can be executed in a controlled manner, for example scheduled for 3 or 4 times in a day. The capability to determine which events should be collected and at which interval they should be exported, lowers the burden of event collection and transfer on both the environment where the events are collected as well as on the event consolidation system thereby improving performance. It allows you to set your own balance between the performance requirement of your systems and the need to collect events.

GUI Based. The product is fully GUI based allowing security officers who are not necessarily "green-screen" experts to easily manage the consolidation and monitoring of sensitive data in their organization .

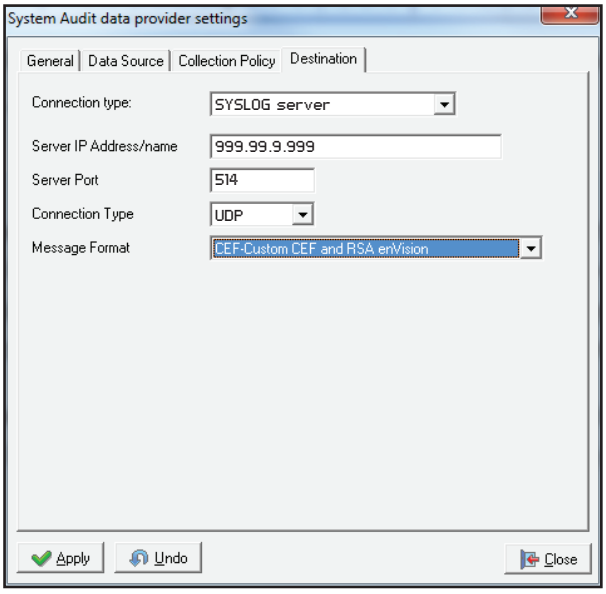

Figure 2: Choosing Destination and Format for System Audit data

About Enforcive, Inc.
Enforcive provides comprehensive security solutions to help businesses reduce workloads, satisfy auditors and improve responsiveness to security threats. For over two decades, Enforcive has been providing solutions within mission critical environments using platforms including IBM i, System z, AIX, Linux and Windows. Our expertise and commitment to innovation enables us to offer the best of breed solutions to our customers.

Enforcive/Enterprise Security for IBM i
Enforcive/Enterprise Security is the single most comprehensive and easy to use security and compliance solution for IBM i. With over twenty fully integrated GUI-controlled security, auditing and compliance modules, this software suite enables system administrators, security officers and auditors to easily manage security and compliance tasks efficiently and effectively.

For more information or to request a free trial:

North America:
Toll Free: 877-237-8024
info@enforcive.com

International:
(+972) 9-9610400
info-eu@enforcive.com