

# Audit

## INTRUSION DETECTION

iSecurity Audit Provides real-time monitoring of system related activities and initiates responses to potential threats. Audit can respond to threats in real-time by triggering alerts and taking immediate corrective action. iSecurity Audit gives organizations the flexibility to audit only the critical events they deem necessary, eliminating the fear of DASD usage. iSecurity Audit's powerful query and report generator provides the data you need in real-time or scheduled through the built in scheduling tool. Audit is available in the native "green-screen" interface or a state-of-the-art GUI version.

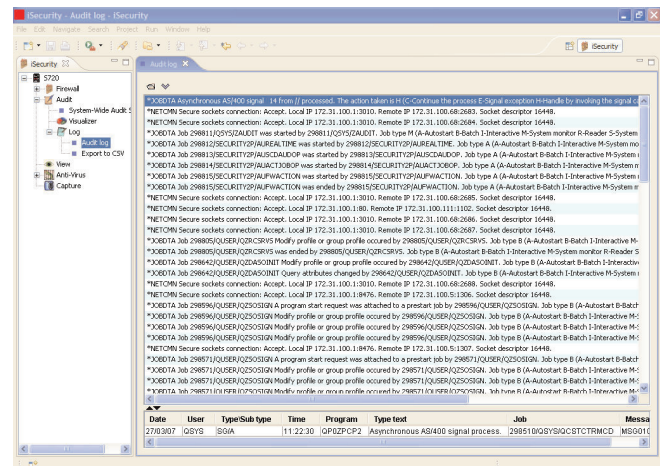
## THE AUDIT SOLUTION

Recent regulations concerning business transparency have placed security auditing as a key component of any organization's IT security program. Simply creating a security policy and purchasing security software tools is not enough. Management must ensure that security policies and procedures are properly implemented and enforced. In addition, managers must be able to evaluate and test the effectiveness of these policies on a continuing basis.

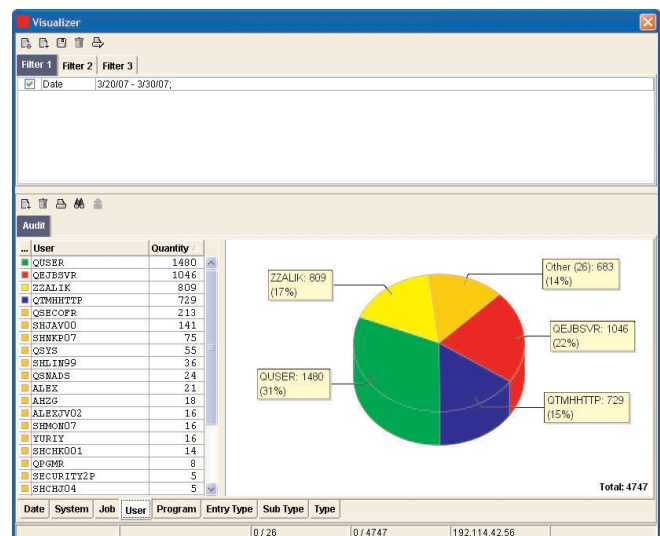
iSecurity Audit solves that problem and more. iSecurity Audit enhances native System i auditing by adding several robust new features, and providing a user-friendly interface for working with the large, often complex, number of system values and parameters. Audit is the only security auditing product available that is designed from the ground up for ease-of-use by non-technical personnel, such as outside auditors and managers. The user interface provides clear explanations for all audit types, parameters, fields and field values.

Audit employs real-time detection to identify security events as they occur and record details in a history log. This log enables you to exploit the powerful query and reporting features that are included with the product. More importantly, real-time detection triggers alerts and/or

takes immediate corrective action. Audit offers the most powerful and flexible reporting features available today. It includes more than eighty ready-to-run queries and reports.



## View specific system audit log information



## Graphically analyze and report on system audit data

The powerful Query Wizard allows users to quickly and easily create audit reports without programming. Queries employ robust selection criteria such as AND/OR, equal/not equal, greater/less than, like/not like, included in list, etc. Only the information that you really need is included. Report formats are fully customizable. In addition, Audit logs display security audit data in a standard message format with the actual data embedded in the message.

## FEATURES

- Monitors user activities and object access in real-time
- Triggers alert messages and corrective action
- Simple to use - no technical knowledge required
- More than eighty pre-defined queries and reports
- Query Wizard - create queries quickly and easily without programming
- Time groups apply rules and filters at predefined times
- "Backward Glance" feature - quickly look at what happened to your system in the last few weeks
- View multiple audit types with one query
- Sort query data in any order
- Design custom output for query data - select and sort data fields
- Report Scheduler - automatically run reports at specified times
- Explanations for parameters and data values are only a keystroke away
- Audit Scheduler - change audit scope automatically at designated times
- Highly sophisticated IDS (Intrusion Detection System) feature to provide real time alerts, warnings and provide corrective actions to threats in real-time
- Built-in business intelligence tool that enables IT managers to graphically analyze security related system activity quickly and easily

## BENEFITS

- Specially designed for non-technical users such as auditors, managers and administrators
- Enables compliance with Sarbanes-Oxley, HIPAA, the California Privacy Act, and more...
- Minimizes throughput delay and resource usage
- Full text explanations of audit types, fields, field values and other data
- Scheduler feature minimizes performance impact during peak periods
- Powerful query and report generator provides the data you need when you need it

```

Work with Real-Time Audit Rules

Real-Time audit rules trigger alerts, responsive actions and event logging.
Select a rule from the list or press F6 to create a new rule.
Subset by entry . . . by description.

Type option, press Enter.
1=Select 3=Copy 4=Delete
Perform

Opt Entry Seq Log Act Rule Description
- AD Y Default for: Auditing changes
- AF Y Default for: Authority failure
- AP Y Default for: Obtaining adopted authority
- AU Y Default for: Attribute change
- Ce Y Default for: User profile changed (Before & After)
- CA Y Default for: Authority changes
- CD Y Default for: Command string audit
- CO Y Default for: Create object
- CP Y Default for: User profile changed, created, or res
- CO Y Default for: Change of *CRQD object
- CU Y Default for: Cluster operations

More...
F3=Exit F6=Add New F8=Print F11=No/Default F12=Cancel F22=Renumbe

```

Specify which audit entry data you want to monitor

**iSecurity**  
System i Security Solutions

IBM Server *Proven*

IBM Business Partner

**SEA**<sup>TM</sup>

**SOFTWARE ENGINEERING OF AMERICA**<sup>®</sup>

Phone: 516.328.7000 • Fax: 516.354.4015 • [www.seasoftware.com](http://www.seasoftware.com)

All trademarks & copyrights are the property of their respective owners.