AUDIT

Auditing, Monitoring and Reporting for IBM i

About Raz-Lee Security

Founded in 1983, Raz-Lee Security is one of the world's leading independent owned cybersecurity and compliance solution providers for IBM i servers (AS/400).

Raz-Lee's flagship iSecurity suite guards organizations against insider threats and unauthorized external access to business-critical information hosted on their IBM i. We have developed cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

We build solutions that work with other companies' technologies allowing organizations to monitor IBM i activity via SIEM or DAM dashboards.

Technology Business Partners

imperva IBM McAfee

Akamai RSA SEA SOFTWARE ENGINEERING OF AMERICA

RAZ-LEE iSecurity

About iSecurity Suite

Advanced Threat Protection

- **Anti-Ransomware**
- **Antivirus** / Malware protection
  - **ICAP** Optional Client/Server for Antivirus

Authentication & Authorization

- **MFA** Multi Factor Authentication
- Self **Password Reset**
- **Authority On Demand**

Protection

- **Firewall** FTP, ODBC…access
- Monitor CL **Commands**
- **Safe-Update** to protect production files

Evaluation, Reporting & Alerts

SIEM & DAM Support

Syslog, SNMP, CEF, LEEF

Visualizer

Business Intelligence for Security

Score Cards

for GDPR, SOX, PCI, HIPAA…

Security Investigator

Data Discovery, Authority Inspector, Assessment

Encryption

- DB2 **Field Encryption** (FIELDPROC)
- **PGP File Encryption**

Data Base Solutions

- **AP-Journal** DB Audit, Filter, Alerts, SIEM
- **DB-Gate** Native SQL to Oracle, MSSQL…
- **FileScope** Secured file editor

Auditing & Response

- **Audit** Journal, System Values, Status…
- Proactive re-**Action** in real time
- **Capture** screen activity
- **Compliance** of Users, Objects, IFS
- **Change Tracker** watch Production Libraries

RAZ-LEE iSecurity

AUDIT

Auditing, Monitoring and Reporting for IBM i

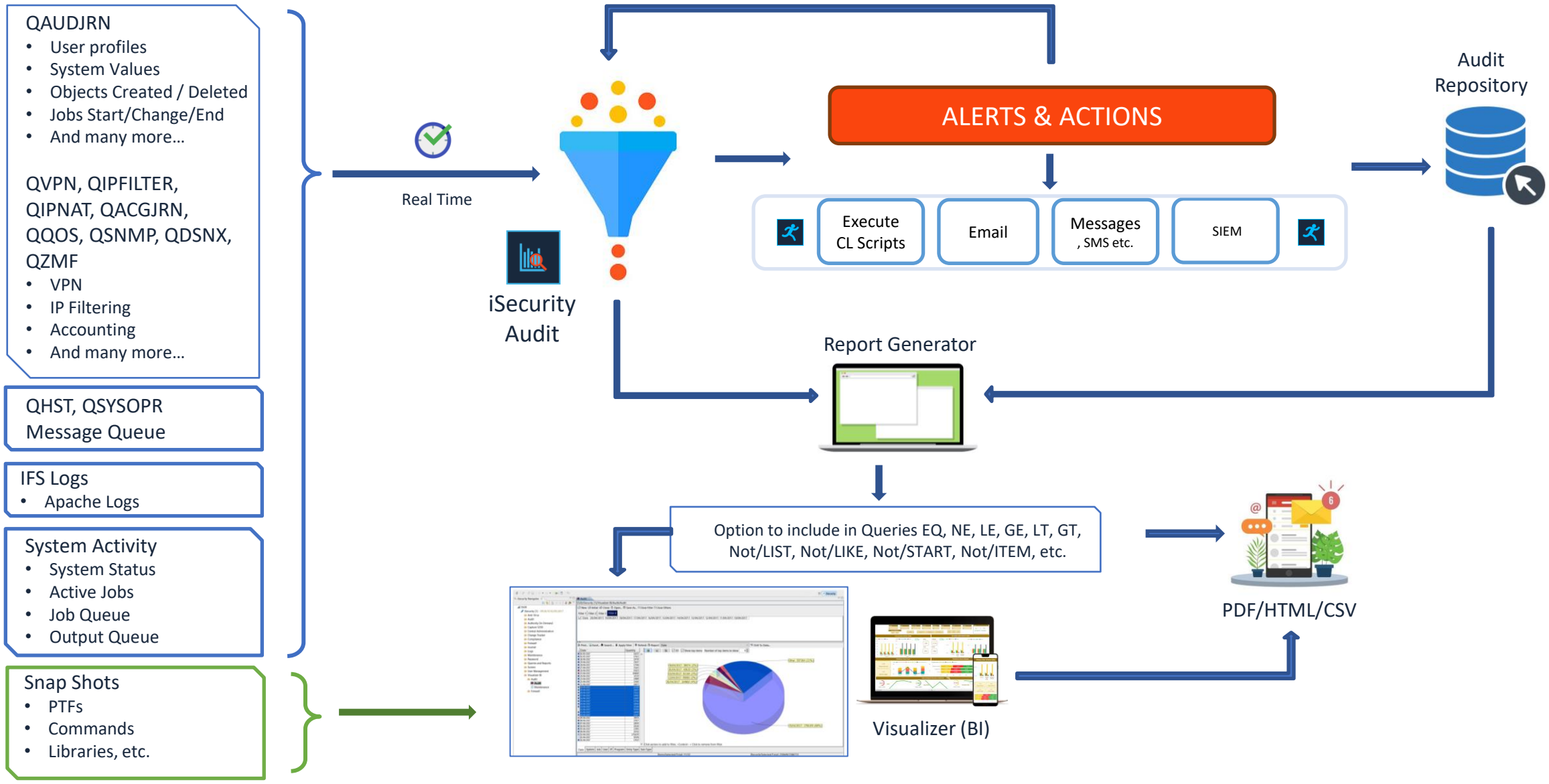
RAZ-LEE iSecurity

The need to Audit

Auditing is a key component of IT security, also regulations concerning Information Security require it due to the following advantages.

- Ensure IT systems are reliable, secure and not vulnerable to computer attacks.
- Reduce risks of data tampering, data loss or leakage, service disruption, and poor management of IT systems.
- GDPR, PCI-DSS, NIS Directive, HIPAA, SOX.
- Event and User Activity Tracking.
- Comply with external auditor's demands.
- Reinforces internal security policies.

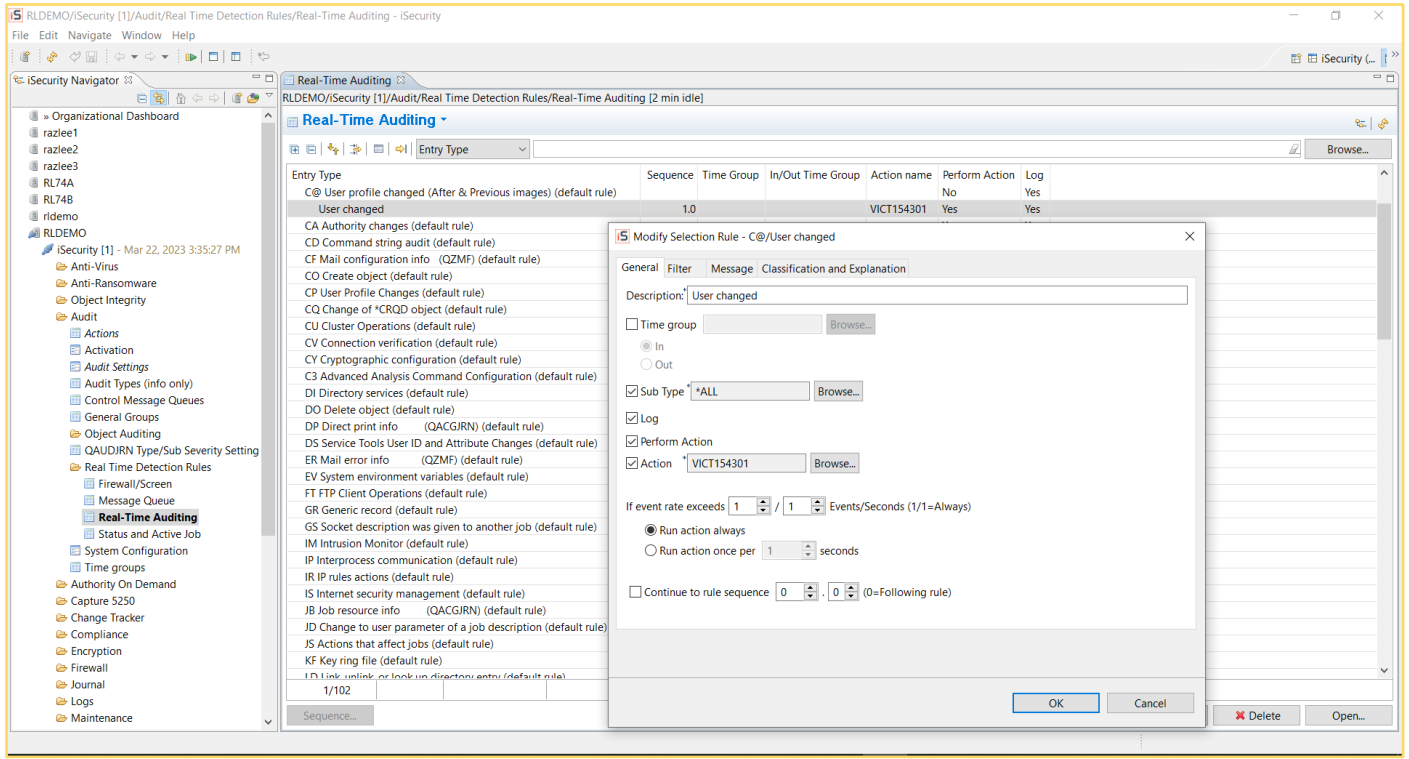
Workflow

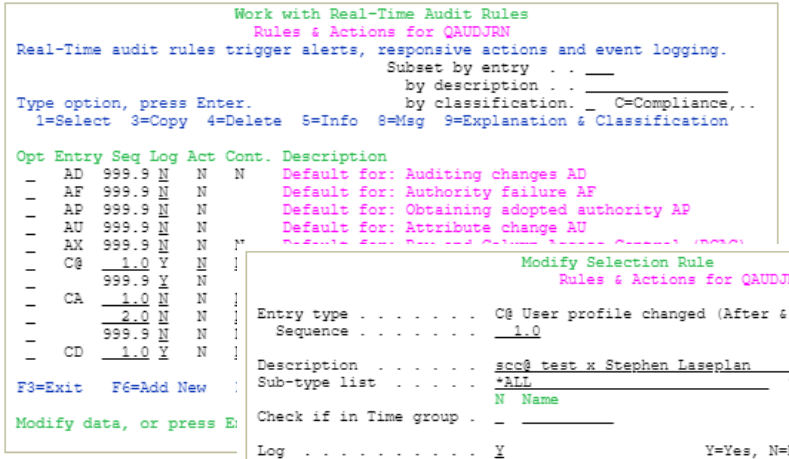

QAUDJRN
• User profiles
• System Values
• Objects Created / Deleted
• Jobs Start/Change/End
• And many more…
QVPN, QIPFILTER, QIPNAT, QACGJRN, QQOS, QSNMP, QDSNX, QZMF
• VPN
• IP Filtering
• Accounting
• And many more…
QHST, QSYSOPR Message Queue
IFS Logs
• Apache Logs
System Activity
• System Status
• Active Jobs
• Job Queue
• Output Queue
Snap Shots
• PTFs
• Commands
• Libraries, etc.
Real Time
iSecurity Audit
ALERTS & ACTIONS
Execute CL Scripts
Email
Messages , SMS etc.
SIEM
Audit Repository
Report Generator
Option to include in Queries EQ, NE, LE, GE, LT, GT, Not/LIST, Not/LIKE, Not/START, Not/ITEM, etc.
PDF/HTML/CSV
Visualizer (BI)

Real-time Detection

Audit examines logs, journals, etc., and respond to security related events in real time.

It uses a powerful filter to examine which events are worth keeping or require reacting, sampling repetitive events and keeping just the essential data.

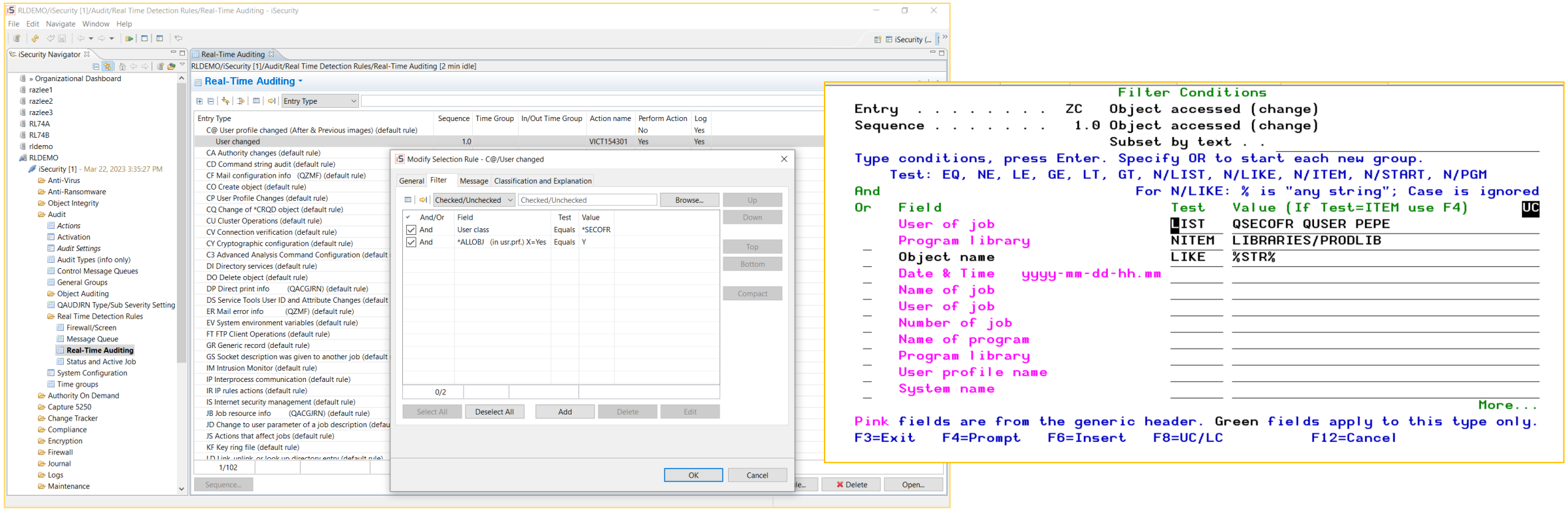




RAZ-LEE iSecurity

The power of Filter

Filter criteria allow you to limit the application of real-time detection rules to certain specific conditions.

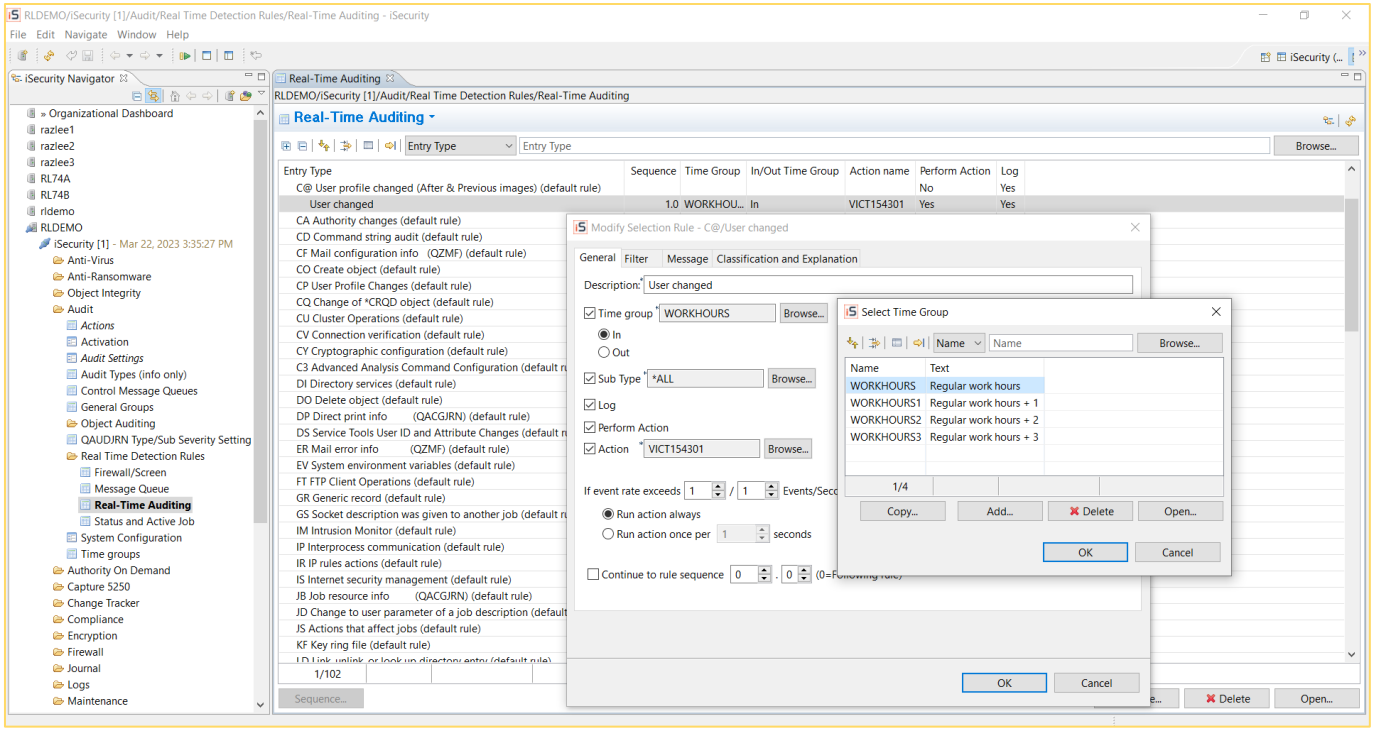


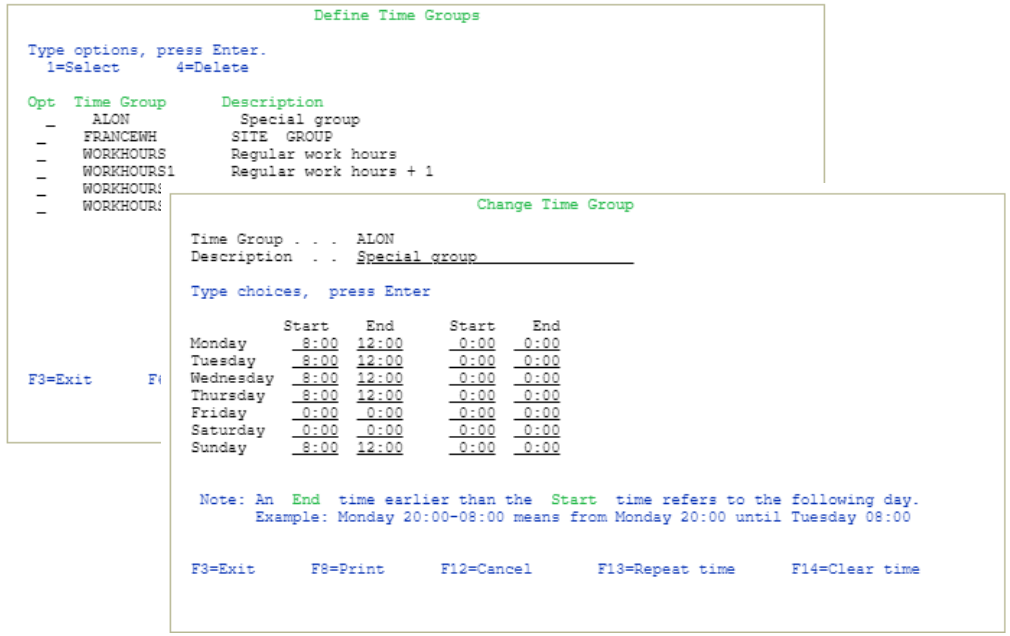
Time Groups

Time groups are user-defined sets of time that can be use as filter criteria for queries, reports and the history log. Time group filters can be either:

Inclusive – Including activities that occur only during the time group periods.

Exclusive – Excluding all activities that occur during the time group periods.





RAZ-LEE iSecurity

Ways to Analyze

The Audit journal is filtered and stored in regular database files (which cannot be overwritten).

Log

- The display log command can show the information in tables structure or as text messages (similar to the standard Display Log or Display Job Log).

Query generator

- Works on the pre-filtered Audit journal info (Authority failures, Creates, Deletes…).
- Works on subjects to be audited (User Profiles, System values, Object authorities…).

Business intelligence

- Data warehouse of statistical info from the Audit journal.
- Result of any report output (or Audit journal or Subjects).

SIEM

- Messages up to 3 SIEM simultaneously.

Report Generation

- Audit offers a powerful and flexible report generator and Scheduler.
- The product comes with an initial set of more than 200 reports which, if needed, can be easily modified as per the customer needs. New reports can be ready in just a few minutes.
- It is used to report information such as: logged events, User profiles, System values, Large objects, etc.
- Report generator output available as Screen, Gui, Print, HTML, PDF, CSV-Excel, etc.
- In a single run it can produce a report and 3 different summary report.
- Keep the data or send them by Email.
- Run over data of any number of LPARs.

Query Wizard

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.

RAZ-LEE iSecurity

iSecurity Audit Advantages

Cutting-edge security auditing application that examines events in real time, and triggers alerts and other responsive actions to potential threats.

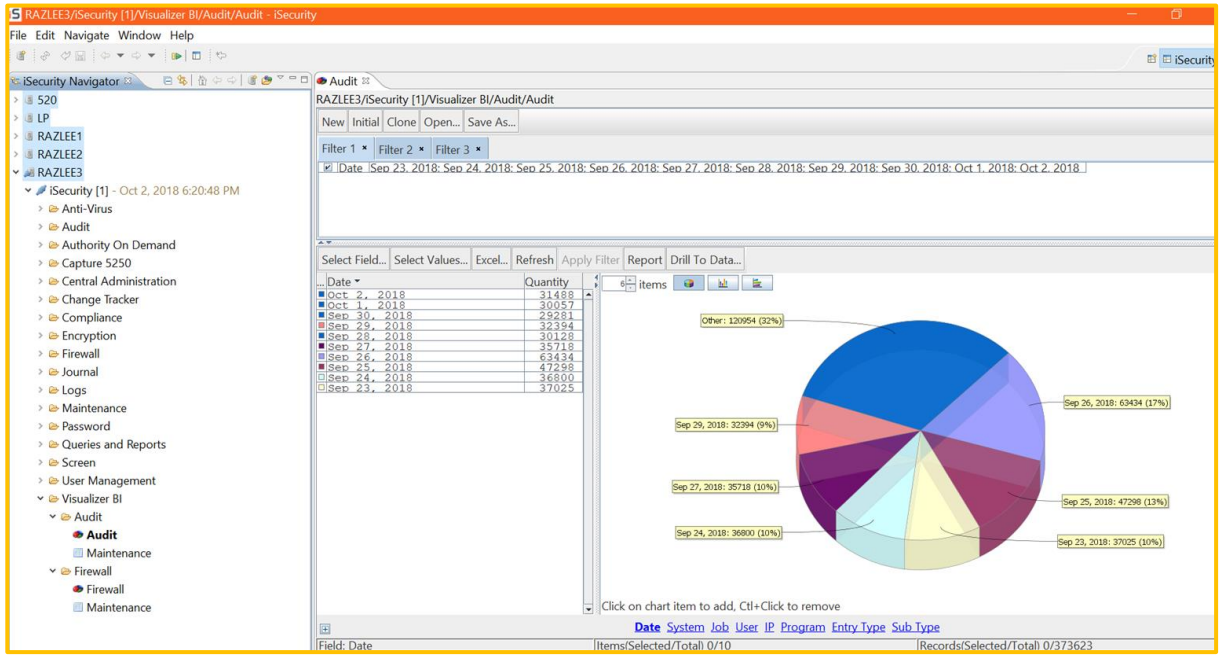
- Specially designed for non-technical users.
- Enables compliance with PCI, GDPR, HIPAA, SOX etc.
- Minimizes throughput delay and resource usage.
- Simple, intuitive audit parameter definition process.
- Full text explanations of audit types, fields, values and other data.
- Powerful query and report generator with Scheduler feature.
- Integrates with **iSecurity Visualizer** to get graphical presentations.

Integrating Visualizer Business Intelligence

A Business Intelligence System for display and analysis of data from the IBM i server.

Allows IT managers and system administrators to graphically analyze IBM i security related activities instantaneously and without OS/400 technical knowledge.

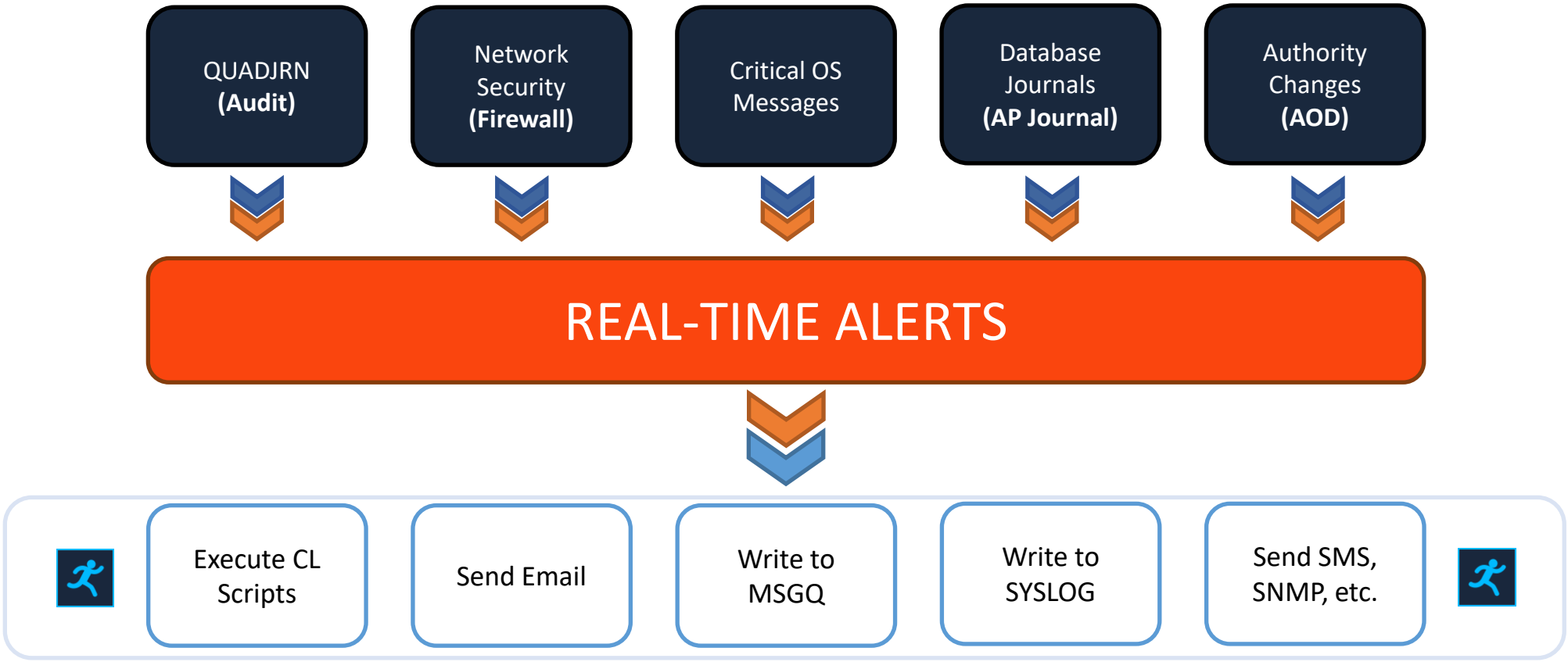
- Graphical presentation and analysis of Firewall, Audit, AP-Journal log data
- Instantaneous response to queries, regardless of log file size
- Excellent for investigative purposes to isolate specific events on specific dates, from certain IP addresses, etc.



RAZ-LEE iSecurity

Integrating Action

Real-time Alert Handling, Manage different actions according to the situation.



RAZ-LEE iSecurity

Summary

- Monitors user activities and object access in real-time.
- Triggers alert messages and corrective actions (**iSecurity Actions**).
- 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 in the last few minutes.
- Sort query data in any order.
- Design custom output for query data.
- Report Scheduler.
- Audit Scheduler.
- Integrated Business Intelligence (**iSecurity Visualizer**).

Thank You

For more information about our company and products please visit

www.razlee.com