RAZ-LEE

iSecurity Audit

iSecurity
Audit

Auditing, Monitoring & Reporting for IBM i

iSecurity Audit Enables compliance with PCI, GDPR, HIPAA, NIS2, DORA, SOX, etc. Reduce risks of data tampering, data loss or leakage, service disruption, and poor management of IT systems.

RAZ-LEE

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.
- ✓ Reduce risks of data tampering, data loss or leakage, service disruption, and poor management of IT systems.
- ✓ **GDPR, PCI-DSS, NIS2, DORA, HIPAA, SOX**, etc. Compliance.
- ✓ Event and User Activity Tracking.
- ✓ Comply with external auditor’s demands.
- ✓ Reinforces internal security policies.

iSecurity Audit Insights

iSecurity Audit examines events in real time, and triggers alerts and other responsive actions to potential threats.

Our Solution:

- ✓ Specially designed for non-technical users.
- ✓ Enables compliance with **PCI, GDPR, HIPAA, NIS2, DORA, SOX**, etc.
- ✓ Minimizes throughput delay and resource usage.
- ✓ Simple, intuitive audit parameter definition process.

iSecurity
Audit

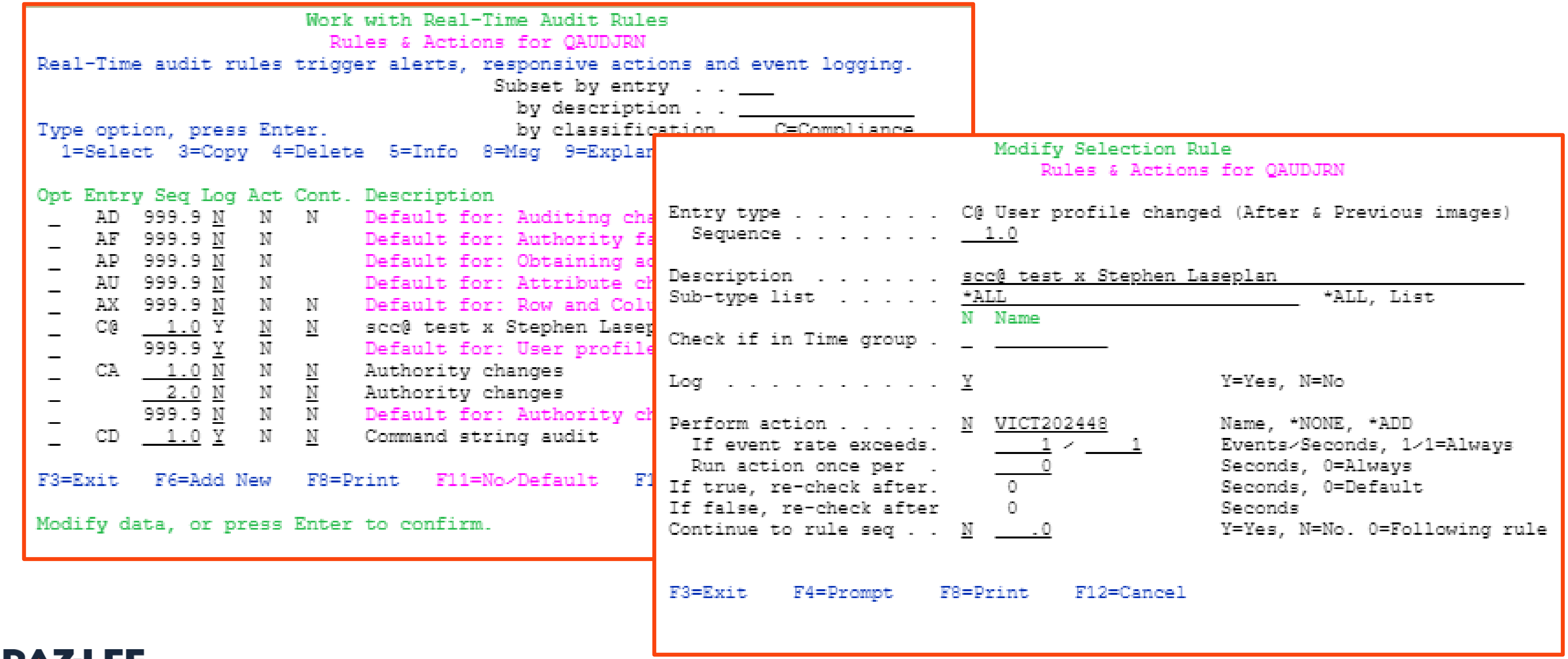
Let’s see our Product in Action!

The best way to see how it works is a demo with **iSecurity Audit** running on a real environment.

RAZ-LEE

Real-time Detection

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



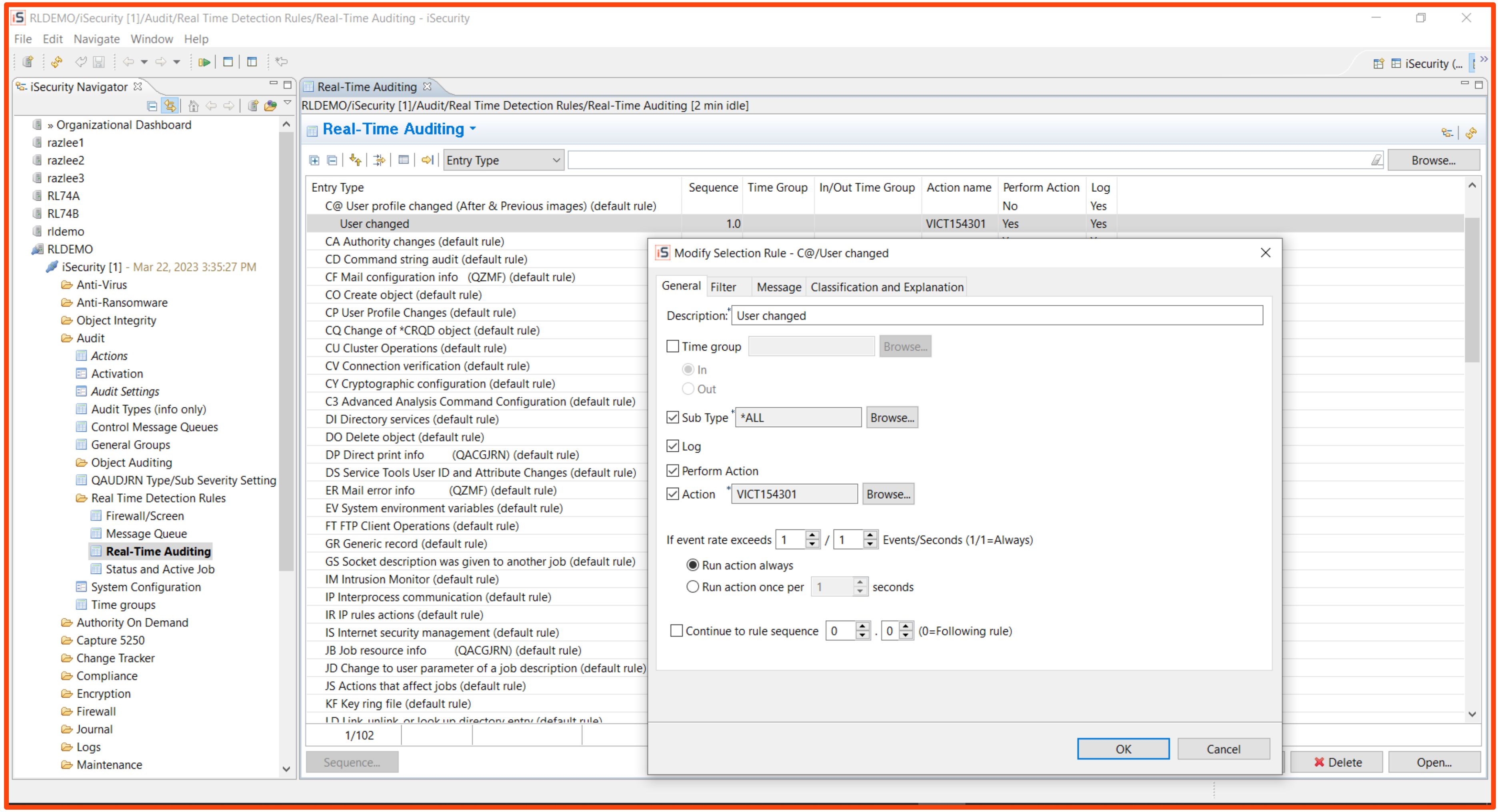
```
                     Work with Real-Time Audit Rules
                       Rules & Actions for QAUDJRN
Real-Time audit rules trigger alerts, responsive actions and event logging.
                                        Subset by entry  . .  ___
                                          by description . .  _______________
Type option, press Enter.                 by classification     C=Compliance
  1=Select   3=Copy   4=Delete   5=Info   8=Msg   9=Explar

Opt Entry Seq   Log  Act Cont. Description
 _   AD   999.9 N    N   N     Default for: Auditing cha
 _   AF   999.9 N    N         Default for: Authority fa
 _   AP   999.9 N    N         Default for: Obtaining ac
 _   AU   999.9 N    N         Default for: Attribute ch
 _   AX   999.9 N    N   N     Default for: Row and Colu
 _   C@     1.0 Y    N   N     scc@ test x Stephen Lasep
 _          999.9 Y  N         Default for: User profile
 _   CA     1.0 N    N   N     Authority changes
 _          2.0 N    N   N     Authority changes
 _          999.9 N  N   N     Default for: Authority ch
 _   CD     1.0 Y    N   N     Command string audit

F3=Exit   F6=Add New   F8=Print   F11=No/Default   F1

Modify data, or press Enter to confirm.
```

```
                       Modify Selection Rule
                        Rules & Actions for QAUDJRN

Entry type . . . . . . . .  C@ User profile changed (After & Previous images)
  Sequence . . . . . . . .    1.0

Description  . . . . . . .  scc@ test x Stephen Laseplan
Sub-type list  . . . . . .  *ALL                          *ALL, List
                            N  Name
Check if in Time group .    _  __________

Log  . . . . . . . . . . .  Y                            Y=Yes, N=No

Perform action . . . . . .  N  VICT202448                Name, *NONE, *ADD
  If event rate exceeds.          1 /      1             Events/Seconds, 1/1=Always
  Run action once per   .         0                      Seconds, 0=Always
If true, re-check after.       0                         Seconds, 0=Default
If false, re-check after       0                         Seconds
Continue to rule seq . .    N     .0                     Y=Yes, N=No. 0=Following rule


F3=Exit    F4=Prompt    F8=Print    F12=Cancel
```

RAZ-LEE iSecurity

Real-time Detection

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



RLDEMO/iSecurity [1]/Audit/Real Time Detection Rules/Real-Time Auditing - iSecurity

File Edit Navigate Window Help

iSecurity Navigator

- » Organizational Dashboard
- razlee1
- razlee2
- razlee3
- RL74A
- RL74B
- rldemo
- RLDEMO
  - iSecurity [1] - Mar 22, 2023 3:35:27 PM
    - Anti-Virus
    - Anti-Ransomware
    - Object Integrity
    - Audit
      - *Actions*
      - Activation
      - *Audit Settings*
      - Audit Types (info only)
      - Control Message Queues
      - General Groups
      - Object Auditing
      - QAUDJRN Type/Sub Severity Setting
      - Real Time Detection Rules
        - Firewall/Screen
        - Message Queue
        - **Real-Time Auditing**
        - Status and Active Job
      - System Configuration
      - Time groups
    - Authority On Demand
    - Capture 5250
    - Change Tracker
    - Compliance
    - Encryption
    - Firewall
    - Journal
    - Logs
    - Maintenance

Real-Time Auditing

RLDEMO/iSecurity [1]/Audit/Real Time Detection Rules/Real-Time Auditing [2 min idle]

Real-Time Auditing

Entry Type | Browse...

Entry Type	Sequence	Time Group	In/Out Time Group	Action name	Perform Action	Log
C@ User profile changed (After & Previous images) (default rule)					No	Yes
User changed	1.0			VICT154301	Yes	Yes
CA Authority changes (default rule)						
CD Command string audit (default rule)						
CF Mail configuration info (QZMF) (default rule)						
CO Create object (default rule)						
CP User Profile Changes (default rule)						
CQ Change of *CRQD object (default rule)						
CU Cluster Operations (default rule)						
CV Connection verification (default rule)						
CY Cryptographic configuration (default rule)						
C3 Advanced Analysis Command Configuration (default rule)						
DI Directory services (default rule)						
DO Delete object (default rule)						
DP Direct print info (QACGJRN) (default rule)						
DS Service Tools User ID and Attribute Changes (default rule)						
ER Mail error info (QZMF) (default rule)						
EV System environment variables (default rule)						
FT FTP Client Operations (default rule)						
GR Generic record (default rule)						
GS Socket description was given to another job (default rule)						
IM Intrusion Monitor (default rule)						
IP Interprocess communication (default rule)						
IR IP rules actions (default rule)						
IS Internet security management (default rule)						
JB Job resource info (QACGJRN) (default rule)						
JD Change to user parameter of a job description (default rule)						
JS Actions that affect jobs (default rule)						
KF Key ring file (default rule)						
LD Link, unlink, or look up directory entry (default rule)						

1/102

Sequence... Delete Open...

Modify Selection Rule - C@/User changed

General | Filter | Message | Classification and Explanation

Description:* User changed

☐ Time group Browse...

○ In

○ Out

☑ Sub Type* *ALL Browse...

☑ Log

☑ Perform Action

☑ Action* VICT154301 Browse...

If event rate exceeds 1 / 1 Events/Seconds (1/1=Always)

● Run action always

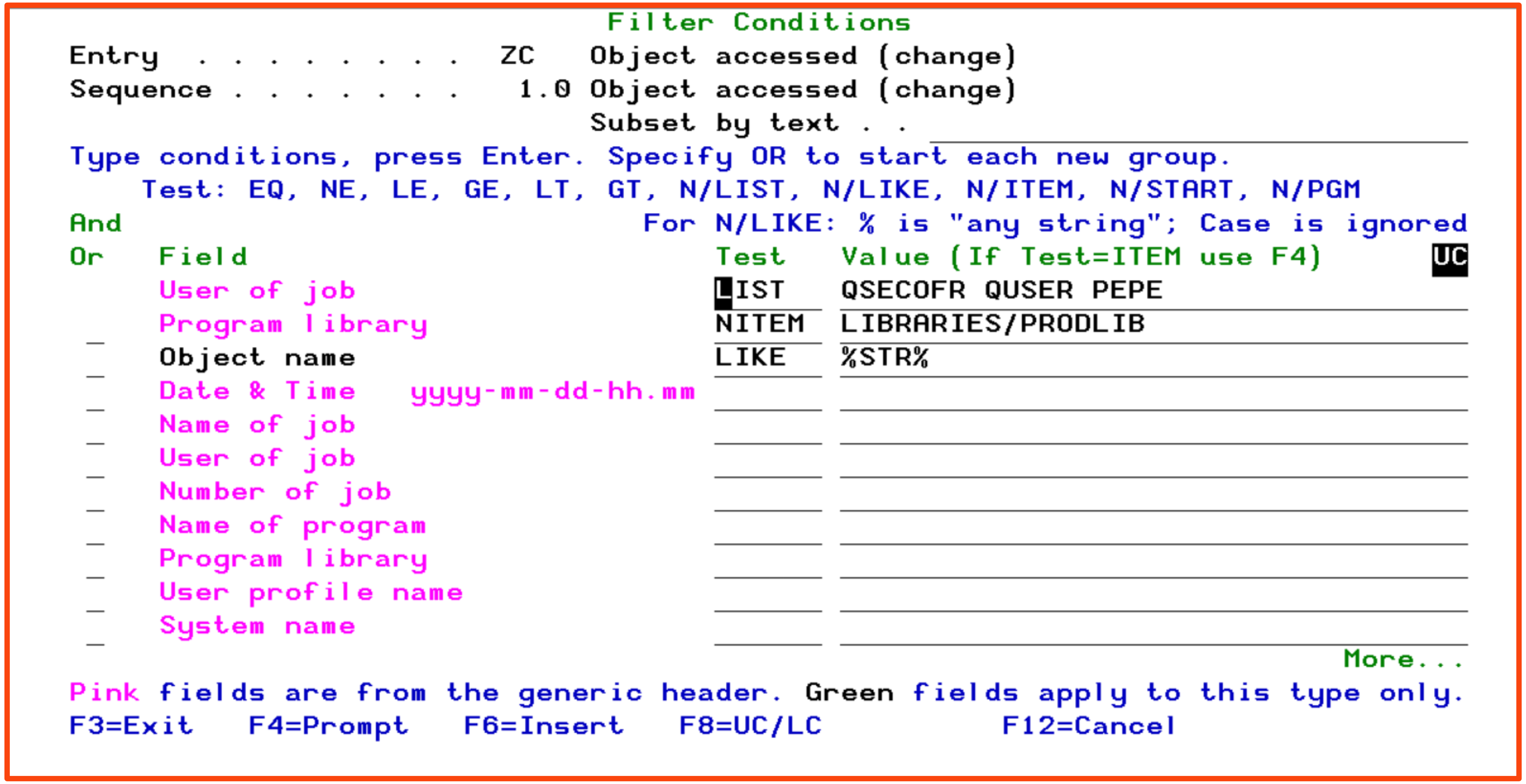
○ Run action once per 1 seconds

☐ Continue to rule sequence 0 . 0 (0=Following rule)

OK Cancel

The power of Filter (Green Screen)

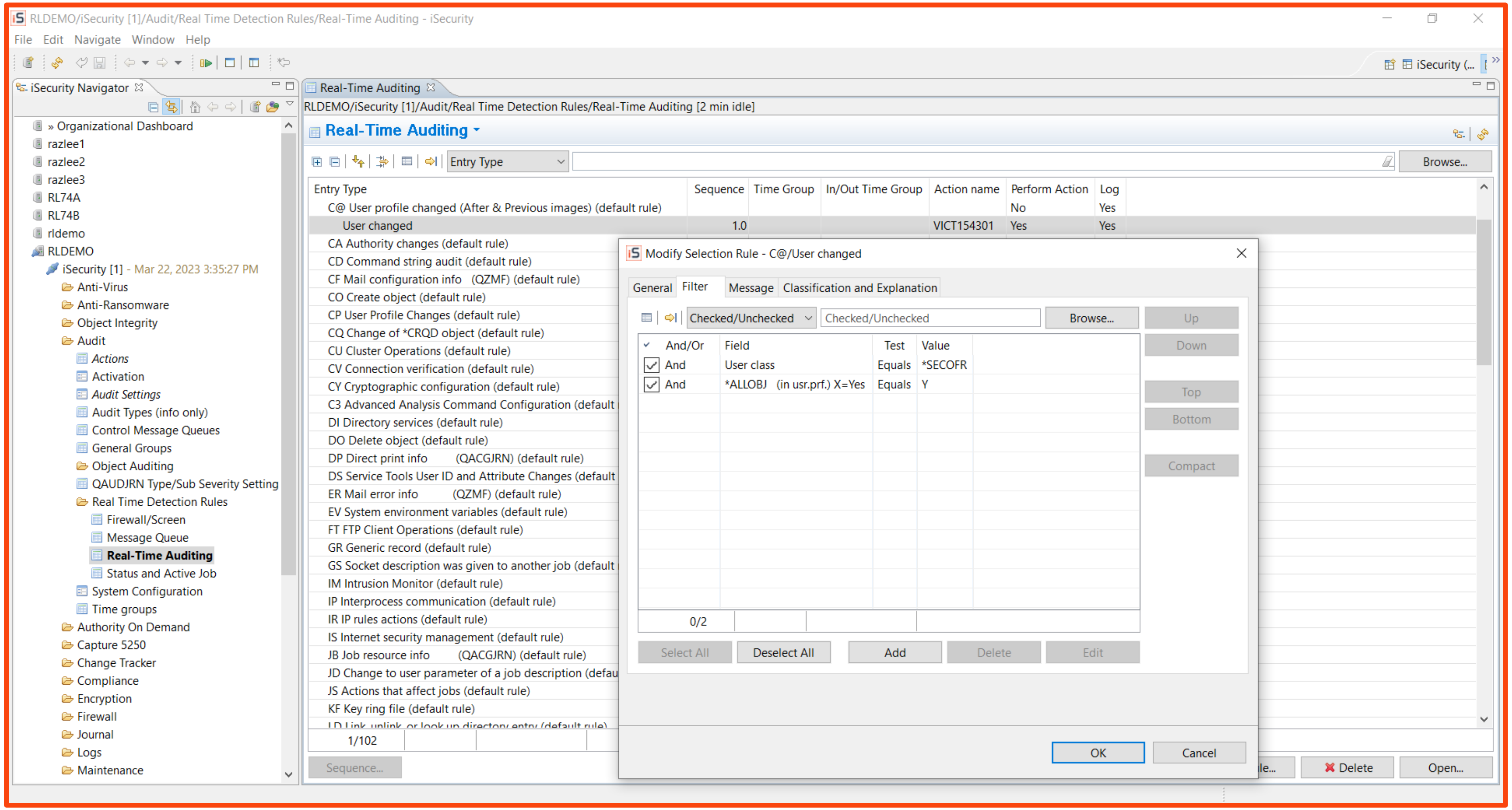
Filter criteria allow you to limit the application of real-time detection rules to certain specific conditions.



```
                              Filter Conditions
Entry  . . . . . . . . .  ZC   Object accessed (change)
Sequence . . . . . . . .   1.0 Object accessed (change)
                               Subset by text . .  ______________________________
Type conditions, press Enter. Specify OR to start each new group.
    Test: EQ, NE, LE, GE, LT, GT, N/LIST, N/LIKE, N/ITEM, N/START, N/PGM
And                              For N/LIKE: % is "any string"; Case is ignored
Or   Field                          Test   Value (If Test=ITEM use F4)         UC
     User of job                    LIST   QSECOFR QUSER PEPE
     Program library                NITEM  LIBRARIES/PRODLIB
 _   Object name                    LIKE   %STR%
 _   Date & Time   yyyy-mm-dd-hh.mm ______ ___________________________________
 _   Name of job                    ______ ___________________________________
 _   User of job                    ______ ___________________________________
 _   Number of job                  ______ ___________________________________
 _   Name of program                ______ ___________________________________
 _   Program library                ______ ___________________________________
 _   User profile name              ______ ___________________________________
 _   System name                    ______ ___________________________________
 _                                  ______ ___________________________________
                                                                         More...
Pink fields are from the generic header. Green fields apply to this type only.
F3=Exit    F4=Prompt    F6=Insert    F8=UC/LC             F12=Cancel
```

The power of Filter (GUI)

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



RLDEMO/iSecurity [1]/Audit/Real Time Detection Rules/Real-Time Auditing - iSecurity

- » Organizational Dashboard
- razlee1
- razlee2
- razlee3
- RL74A
- RL74B
- rldemo
- RLDEMO
  - iSecurity [1] - Mar 22, 2023 3:35:27 PM
    - Anti-Virus
    - Anti-Ransomware
    - Object Integrity
    - Audit
      - *Actions*
      - Activation
      - *Audit Settings*
      - Audit Types (info only)
      - Control Message Queues
      - General Groups
      - Object Auditing
      - QAUDJRN Type/Sub Severity Setting
      - Real Time Detection Rules
        - Firewall/Screen
        - Message Queue
        - **Real-Time Auditing**
        - Status and Active Job
      - System Configuration
      - Time groups
    - Authority On Demand
    - Capture 5250
    - Change Tracker
    - Compliance
    - Encryption
    - Firewall
    - Journal
    - Logs
    - Maintenance

RLDEMO/iSecurity [1]/Audit/Real Time Detection Rules/Real-Time Auditing [2 min idle]

Real-Time Auditing

Entry Type	Sequence	Time Group	In/Out Time Group	Action name	Perform Action	Log
C@ User profile changed (After & Previous images) (default rule)					No	Yes
User changed	1.0			VICT154301	Yes	Yes
CA Authority changes (default rule)						
CD Command string audit (default rule)						
CF Mail configuration info (QZMF) (default rule)						
CO Create object (default rule)						
CP User Profile Changes (default rule)						
CQ Change of *CRQD object (default rule)						
CU Cluster Operations (default rule)						
CV Connection verification (default rule)						
CY Cryptographic configuration (default rule)						
C3 Advanced Analysis Command Configuration (default						
DI Directory services (default rule)						
DO Delete object (default rule)						
DP Direct print info (QACGJRN) (default rule)						
DS Service Tools User ID and Attribute Changes (default						
ER Mail error info (QZMF) (default rule)						
EV System environment variables (default rule)						
FT FTP Client Operations (default rule)						
GR Generic record (default rule)						
GS Socket description was given to another job (default						
IM Intrusion Monitor (default rule)						
IP Interprocess communication (default rule)						
IR IP rules actions (default rule)						
IS Internet security management (default rule)						
JB Job resource info (QACGJRN) (default rule)						
JD Change to user parameter of a job description (defau						
JS Actions that affect jobs (default rule)						
KF Key ring file (default rule)						
LD Link, unlink, or look up directory entry (default rule)						

1/102

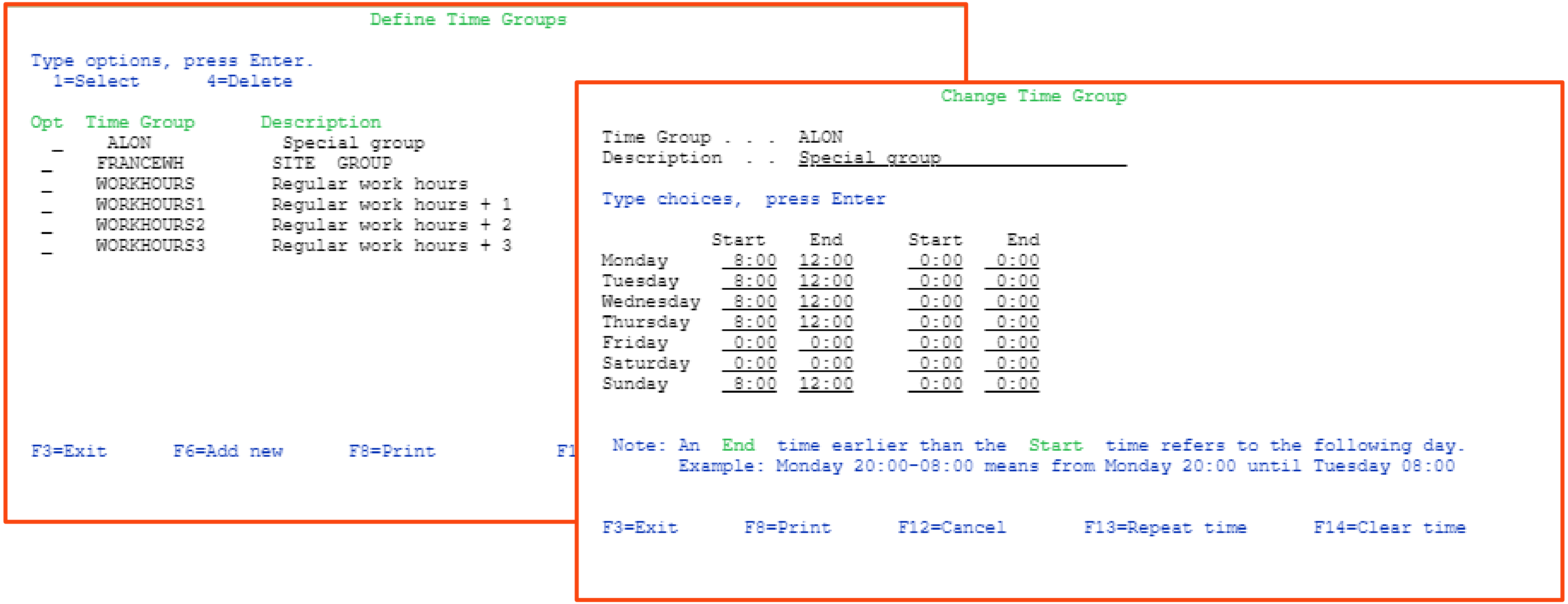
Modify Selection Rule - C@/User changed

✓	And/Or	Field	Test	Value
☑	And	User class	Equals	*SECOFR
☑	And	*ALLOBJ (in usr.prf.) X=Yes	Equals	Y

0/2

Time Groups (Green Screen)

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



```
                         Define Time Groups

Type options, press Enter.
  1=Select      4=Delete

Opt  Time Group       Description
 _     ALON             Special group
 _    FRANCEWH         SITE  GROUP
 _    WORKHOURS        Regular work hours
 _    WORKHOURS1       Regular work hours + 1
 _    WORKHOURS2       Regular work hours + 2
 _    WORKHOURS3       Regular work hours + 3



F3=Exit      F6=Add new      F8=Print            F1
```

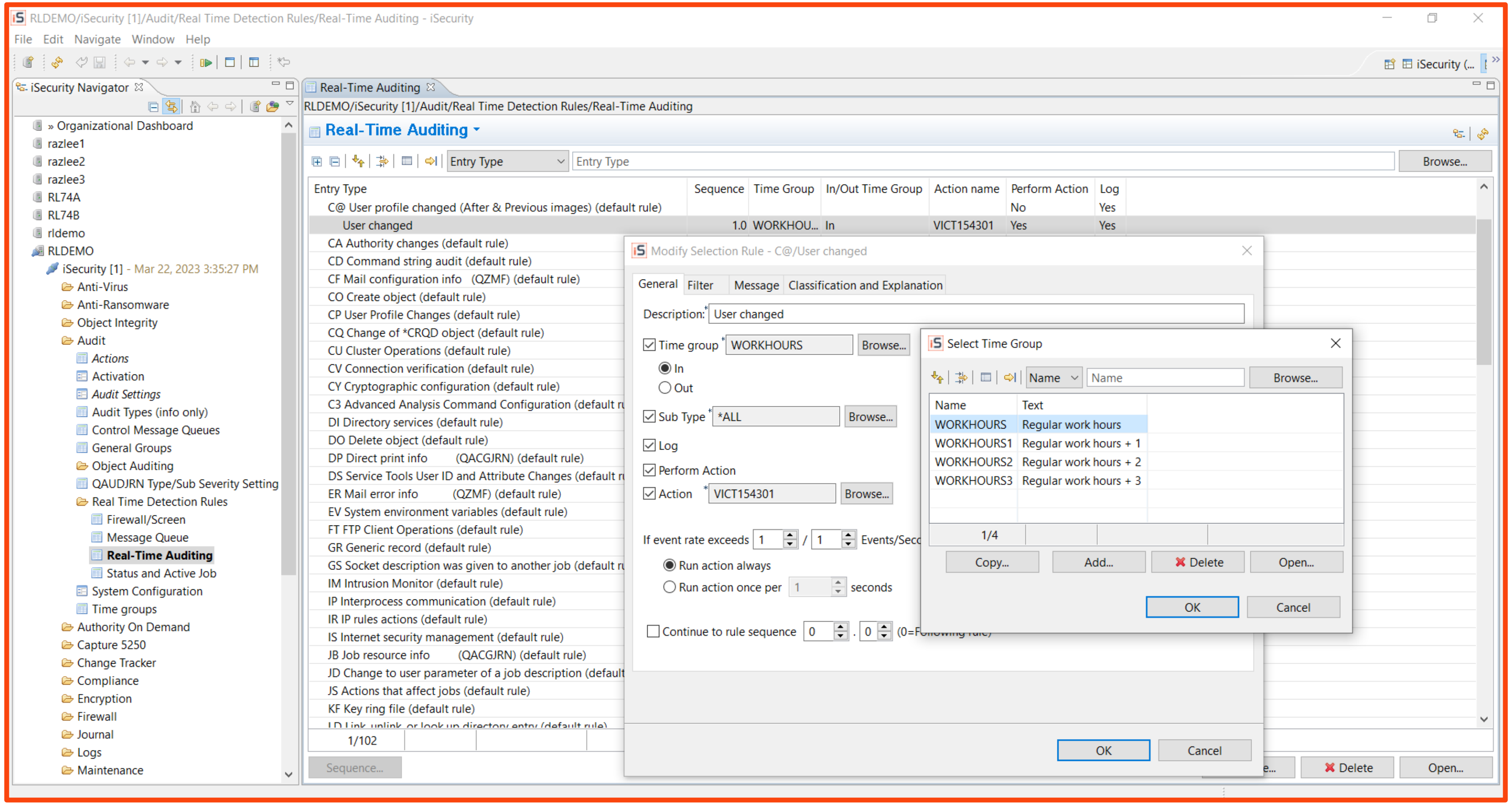
```
                             Change Time Group

Time Group . . .   ALON
Description  . .   Special group

Type choices,  press Enter

            Start    End         Start    End
Monday       8:00   12:00         0:00    0:00
Tuesday      8:00   12:00         0:00    0:00
Wednesday    8:00   12:00         0:00    0:00
Thursday     8:00   12:00         0:00    0:00
Friday       0:00    0:00         0:00    0:00
Saturday     0:00    0:00         0:00    0:00
Sunday       8:00   12:00         0:00    0:00


 Note: An  End  time earlier than the  Start  time refers to the following day.
       Example: Monday 20:00-08:00 means from Monday 20:00 until Tuesday 08:00


F3=Exit      F8=Print      F12=Cancel      F13=Repeat time      F14=Clear time
```

RAZ-LEE
iSecurity

Time Groups (GUI)

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.



RLDEMO/iSecurity [1]/Audit/Real Time Detection Rules/Real-Time Auditing - iSecurity

iSecurity Navigator:

- » Organizational Dashboard
- razlee1
- razlee2
- razlee3
- RL74A
- RL74B
- rldemo
- RLDEMO
  - iSecurity [1] - Mar 22, 2023 3:35:27 PM
    - Anti-Virus
    - Anti-Ransomware
    - Object Integrity
    - Audit
      - Actions
      - Activation
      - Audit Settings
      - Audit Types (info only)
      - Control Message Queues
      - General Groups
      - Object Auditing
      - QAUDJRN Type/Sub Severity Setting
      - Real Time Detection Rules
        - Firewall/Screen
        - Message Queue
        - **Real-Time Auditing**
        - Status and Active Job
      - System Configuration
      - Time groups
    - Authority On Demand
    - Capture 5250
    - Change Tracker
    - Compliance
    - Encryption
    - Firewall
    - Journal
    - Logs
    - Maintenance

RLDEMO/iSecurity [1]/Audit/Real Time Detection Rules/Real-Time Auditing

Real-Time Auditing

Entry Type | Entry Type | Browse...

Entry Type	Sequence	Time Group	In/Out Time Group	Action name	Perform Action	Log
C@ User profile changed (After & Previous images) (default rule)					No	Yes
User changed	1.0	WORKHOU...	In	VICT154301	Yes	Yes
CA Authority changes (default rule)						
CD Command string audit (default rule)						
CF Mail configuration info (QZMF) (default rule)						
CO Create object (default rule)						
CP User Profile Changes (default rule)						
CQ Change of *CRQD object (default rule)						
CU Cluster Operations (default rule)						
CV Connection verification (default rule)						
CY Cryptographic configuration (default rule)						
C3 Advanced Analysis Command Configuration (default ru						
DI Directory services (default rule)						
DO Delete object (default rule)						
DP Direct print info (QACGJRN) (default rule)						
DS Service Tools User ID and Attribute Changes (default ru						
ER Mail error info (QZMF) (default rule)						
EV System environment variables (default rule)						
FT FTP Client Operations (default rule)						
GR Generic record (default rule)						
GS Socket description was given to another job (default ru						
IM Intrusion Monitor (default rule)						
IP Interprocess communication (default rule)						
IR IP rules actions (default rule)						
IS Internet security management (default rule)						
JB Job resource info (QACGJRN) (default rule)						
JD Change to user parameter of a job description (default						
JS Actions that affect jobs (default rule)						
KF Key ring file (default rule)						
LD Link, unlink, or look up directory entry (default rule)						

1/102

Sequence... | e... | ✖ Delete | Open...

Modify Selection Rule - C@/User changed

General | Filter | Message | Classification and Explanation

Description:* User changed

☑ Time group* WORKHOURS Browse...

● In
○ Out

☑ Sub Type* *ALL Browse...

☑ Log

☑ Perform Action

☑ Action* VICT154301 Browse...

If event rate exceeds 1 / 1 Events/Sec

● Run action always
○ Run action once per 1 seconds

☐ Continue to rule sequence 0 . 0 (0=Following rule)

OK | Cancel

Select Time Group

Name | Name | Browse...

Name	Text
WORKHOURS	Regular work hours
WORKHOURS1	Regular work hours + 1
WORKHOURS2	Regular work hours + 2
WORKHOURS3	Regular work hours + 3

1/4

Copy... | Add... | ✖ Delete | Open...

OK | Cancel

Advantages on our Solution

iSecurity Audit offers a powerful and flexible report generator and Scheduler. **Query Wizard** create queries quickly and easily without programming.

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…).

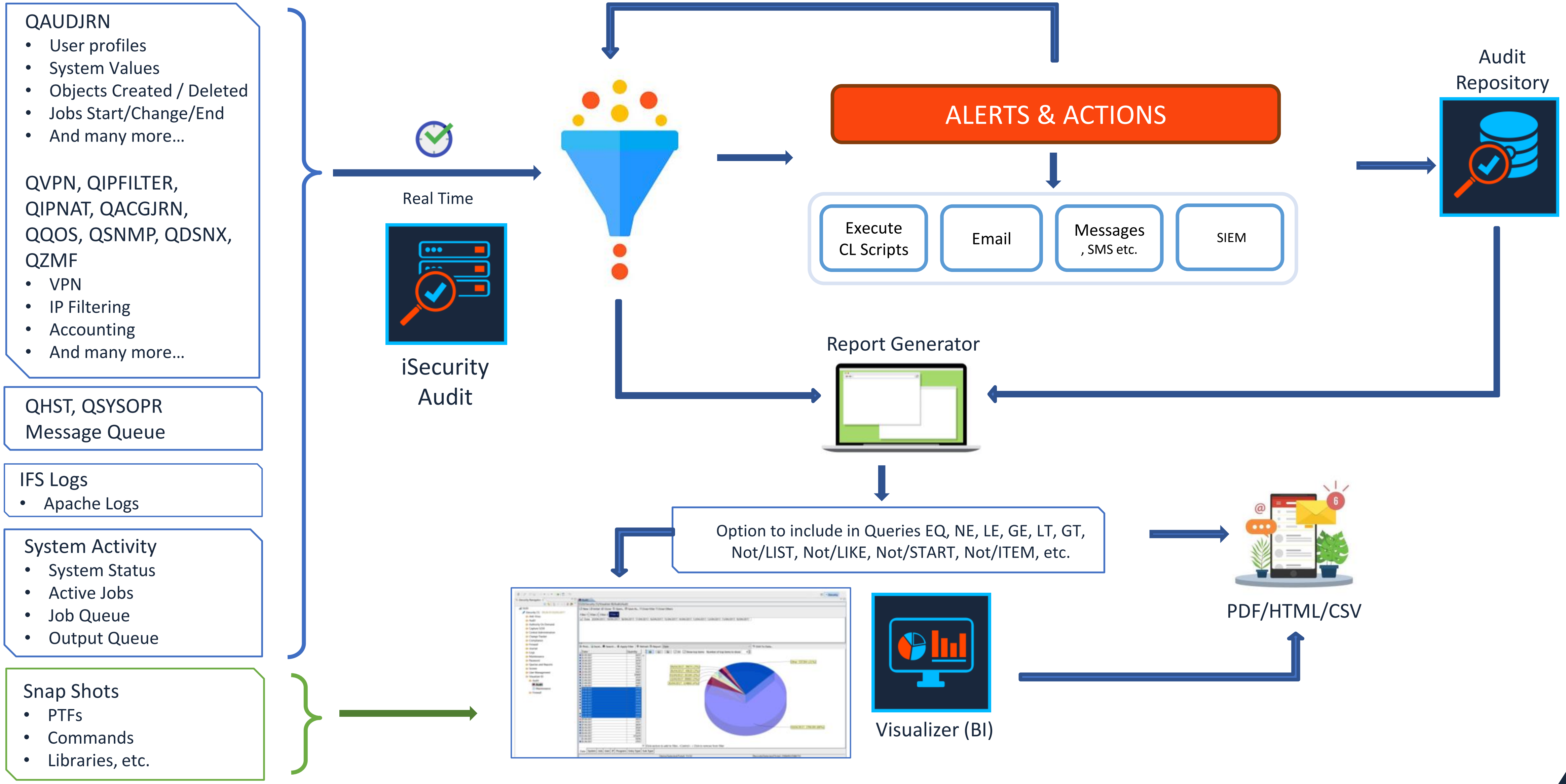
Business intelligence

- 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.

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.

Visualizer (BI)

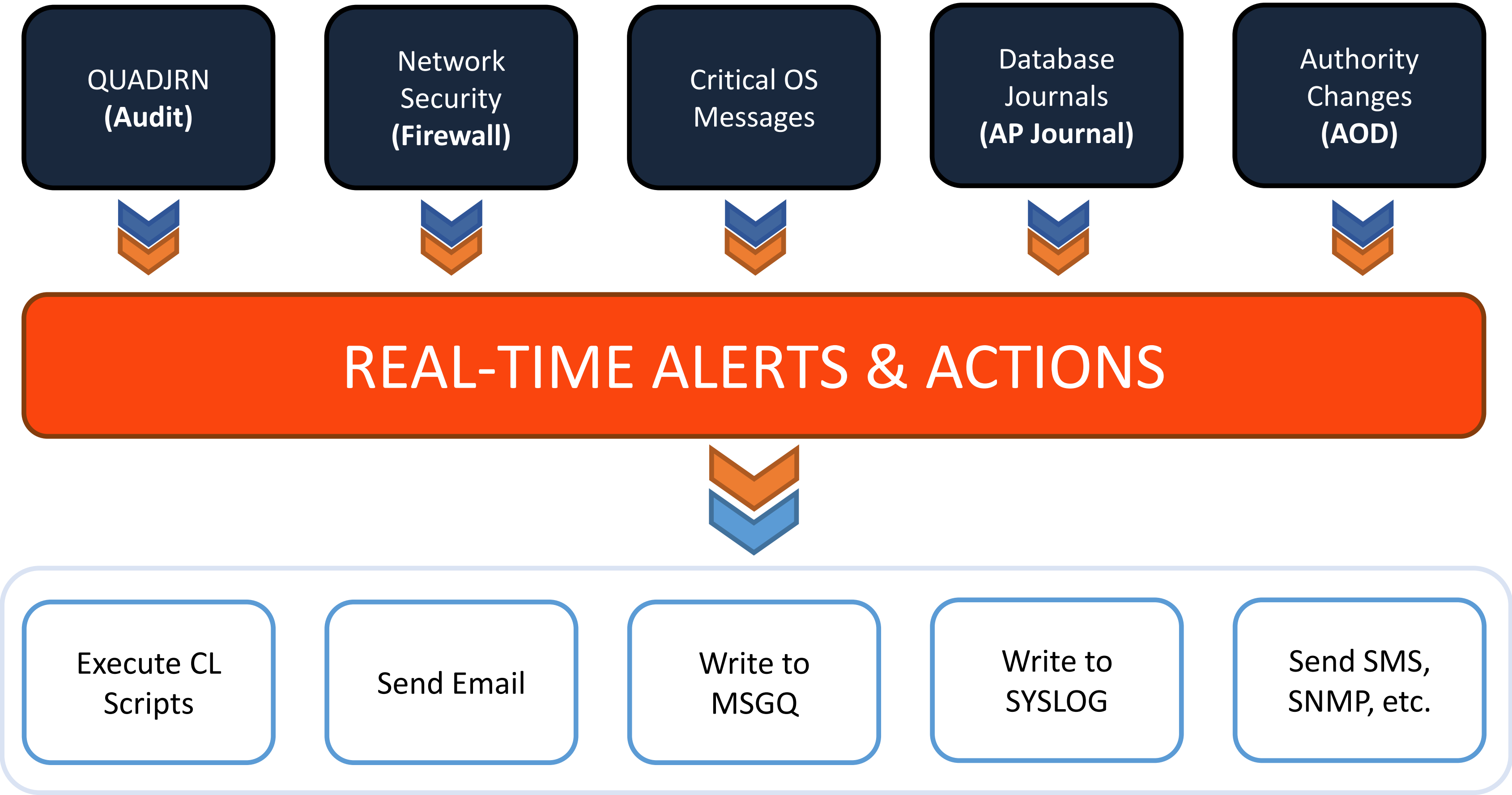
PDF/HTML/CSV

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.

Integrating Action

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



QUADJRN **(Audit)**

Network Security **(Firewall)**

Critical OS Messages

Database Journals **(AP Journal)**

Authority Changes **(AOD)**

REAL-TIME ALERTS & ACTIONS

Execute CL Scripts

Send Email

Write to MSGQ

Write to SYSLOG

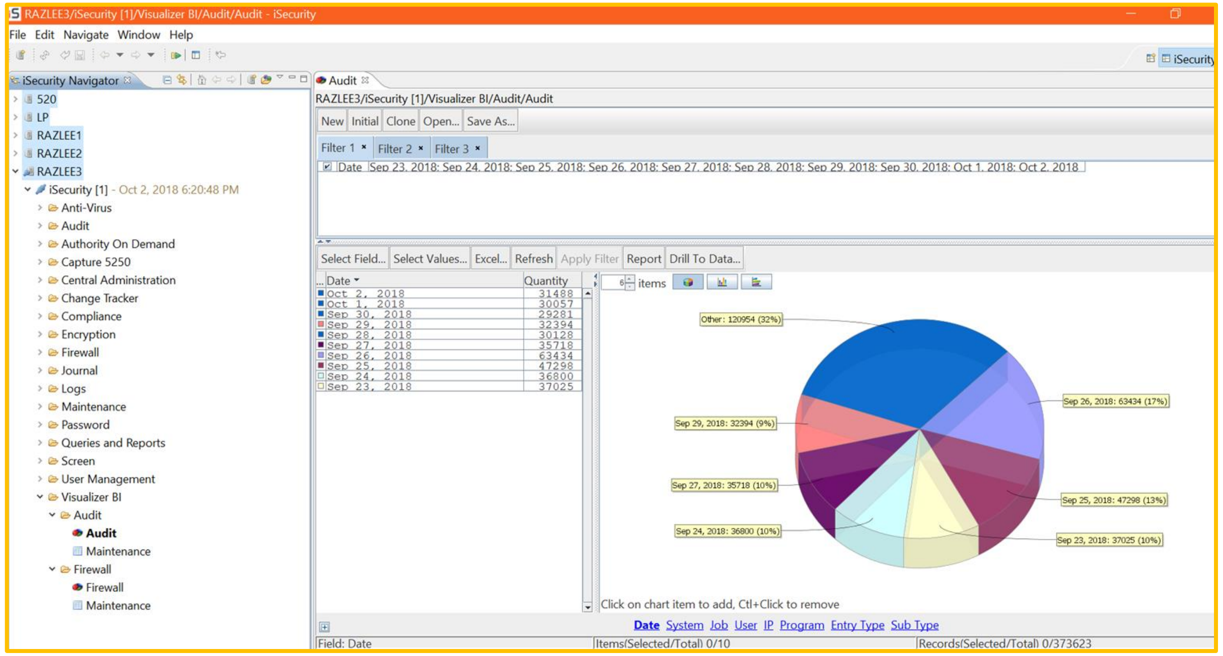
Send SMS, SNMP, etc.

Integrating Visualizer Business Intelligence

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

IT managers and system administrators can 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.



RAZLEE3/iSecurity [1]/Visualizer BI/Audit/Audit

☑ Date Sep 23, 2018: Sep 24, 2018: Sep 25, 2018: Sep 26, 2018: Sep 27, 2018: Sep 28, 2018: Sep 29, 2018: Sep 30, 2018: Oct 1, 2018: Oct 2, 2018

...	Date	Quantity
■	Oct 2, 2018	31488
■	Oct 1, 2018	30057
■	Sep 30, 2018	29281
■	Sep 29, 2018	32394
■	Sep 28, 2018	30128
■	Sep 27, 2018	35718
■	Sep 26, 2018	63434
■	Sep 25, 2018	47298
□	Sep 24, 2018	36800
□	Sep 23, 2018	37025

Click on chart item to add, Ctl+Click to remove

Field: Date | Items(Selected/Total) 0/10 | Records(Selected/Total) 0/373623

RAZ-LEE iSecurity

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, equal /not, greater/less than, like/not like, included in list, etc.
- ✓ Only the information that you really need is included.
- ✓ Report formats are fully customizable.
- ✓ Report Scheduler.
- ✓ Audit Scheduler.
- ✓ Integrated Business Intelligence (**iSecurity Visualizer**).

iSecurity Audit Advantages

- ✓ Specially designed for non-technical users.
- ✓ Enables compliance with **PCI, GDPR, HIPAA, NIS2, DORA, 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.
- ✓ **Query Wizard** create queries quickly and easily without programming.
- ✓ Powerful query and report generator with Scheduler feature.
- ✓ Monitors user activities and object access in real-time.
- ✓ Triggers alert messages and corrective actions (**iSecurity Action**).
- ✓ Integrated Business Intelligence (**iSecurity Visualizer**).
- ✓ Time groups apply rules and filters at predefined times.
- ✓ Backward Glance feature quickly look at what happened in the last few minutes.

RAZ-LEE
iSecurity

RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com

iSecurity Audit