

RAZ-LEE

iSecurity
Action



iSecurity
Action

Security Breach Response & Corrections

iSecurity Action brings Proactive Response in real-time to any security event by Email, SMS, Syslog, SNMP, and CL script processor.

Taking Action in Real Time

In today's business environment, it is not enough to discover and report on a security problem after it occurs.

- ✓ Traditional audit software provides useful historical data after the fact but often lacks state-of-the-art functionality to provide relevant managers with alerts and enable corrective specific corrective actions.
- ✓ **iSecurity Action** provides a comprehensive, easy-to-use solution. For example, if a user attempts to copy a critical file, Action can send an SMS message to the security officer's mobile phone and automatically sign off and disable the offending user. Scripts can even initiate actions that execute if an appropriate response does not occur within a specified period of time!



iSecurity Action Insights

iSecurity Action real-time detection continuously monitors the system for a wide variety of security and other system events

Our Solution reacts to:

- ✓ Events detected by **Audit** real-time auditing.
- ✓ Transactions detected by **Firewall** network security rules.
- ✓ Viruses detected by **Antivirus**.
- ✓ Suspicious data changes by **AP-Journal**.
- ✓ Active job status and checking for jobs that are not active.
- ✓ Current system and memory pool status.



iSecurity
Action

Let's see our Product in Action!

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



RAZ-LEE

Action Start Screen (Native Interface)

```
AUACTMN                                     Action                                     iSecurity/Action
                                                                                               System:  RLDEMO
Select one of the following:

Settings
  1. Activate Real-Time Detection

Real-Time Detection Rules
  11. Real Time Auditing (Audit)
  12. Firewall/Screen (Firewall)
  13. Status & Active Job (SysCtl)
  14. Message Queue          (SysCtl)

Control Features
  21. User Management
  22. Authority Adoption
  23. Object Integrity

Selection or command
===> _____

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant   F16=System main menu
```

Defining Action that Sends Email and Blocks a User (GUI)

The screenshot displays the iSecurity Navigator interface with the 'Actions' list. A table of actions is shown, with 'VICTOR' selected. Two dialog boxes are overlaid on the screen, illustrating the configuration steps:

- Dialog 1 (VICTOR - Edit):** Shows the 'General' tab with 'Description: Email to Victor' and 'Message ID: Automatic' selected.
- Dialog 2 (VICTOR - Edit):** Shows the 'Send To' tab with a table of recipients:

Address	Type
VV	E-mail
VICTOR	Message Queue
3	SIEM

Dialog 3 (VICTOR - Edit): Shows the 'Command Script' tab with a table of commands:

Label	Command	On Error
	CHGUSRPRF USRPRF(&C@USER &C@UPRF) STATUS(*DISABLED)	

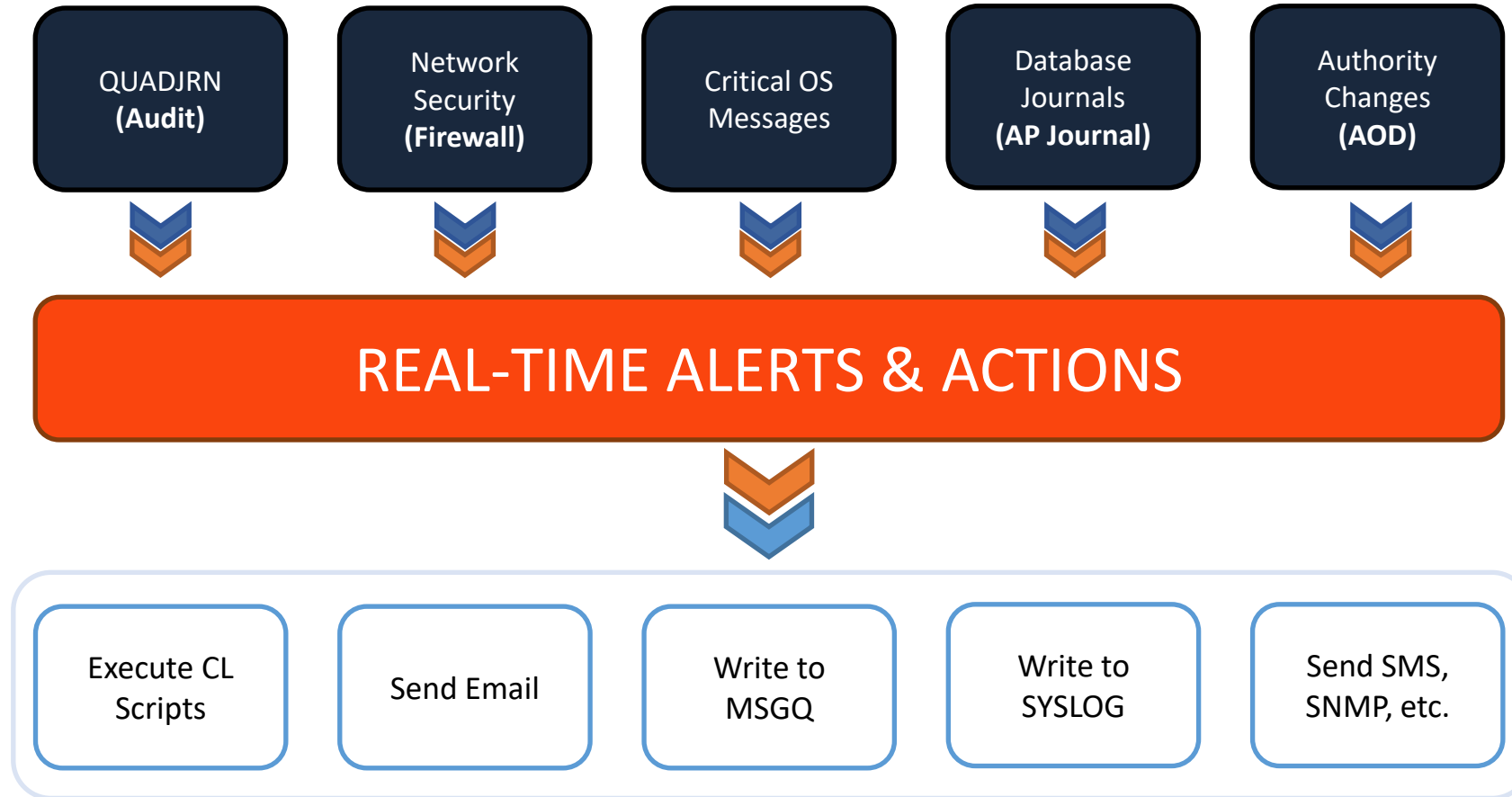
| Advantages on our Solution

iSecurity Action Responds to events detected by other iSecurity Modules like **Audit, Firewall, AP-Journal, Antivirus, Authority on Demand**, etc.



Workflow

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



Rule Wizard

It is extremely easy to define rules and actions with the Action Rule Wizard feature.

- ✓ **Rules trigger** actions and alerts based on one or more parameters associated with a particular event. Examples of selection parameters include user, date, time, job, workstation, library, object name, IP address, command, job name, etc.
- ✓ **Rule criteria** use many different Boolean operators such as: equal/not equal, greater than /less than, like/not like, “contained in list”, “starts with”, etc., and even Group/Item. For example, “NE ALLUSERS/MANAGER” would filter events which were initiated by a non-manager! No other security alert/action system offers such power and flexibility.
- ✓ **Action includes** additional security features such as automatic disabling of inactive users, restricting user access during planned absences and control over creating and running programs that use adopted authority.



iSecurity Action Advantages

- ✓ Responds to events detected by **Audit, Firewall, AP-Journal, Antivirus, Authority on Demand**, etc.
- ✓ Alert messages sent via Syslog, SNMP, e-mail, SMS, MSGQ or Twitter.
- ✓ Automatically takes corrective actions by running command scripts or programs.
- ✓ Rule Wizard makes definition process simple for non-technical users.
- ✓ Rules can use many different selection criteria.
- ✓ Built-in command script interpreter with replacement variable support.
- ✓ Responds to current system status parameters and active jobs.
- ✓ Restrict user access during vacations, holidays and other planned absences.
- ✓ Automatically disables inactive user profiles.
- ✓ Tight control over authority adoption.



RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com

iSecurity
Action

