

Action

Overview

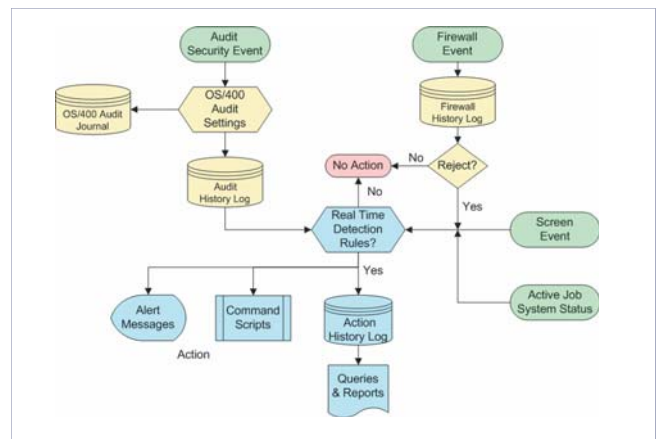
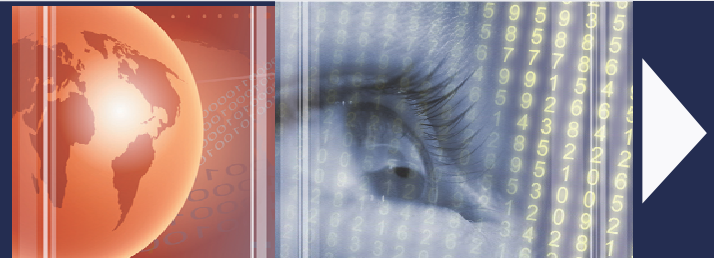
Action is a powerful security solution that intercepts security breaches and other events in real-time and immediately takes appropriate corrective action. Actions may include sending alert messages to key personnel and/or running command scripts or programs that take corrective steps.

The Action Solution

In today's business environment, it is no longer sufficient to discover a security problem after it occurs. Traditional audit software provides useful historical data after the fact. This is the digital equivalent of closing the barn door after the horses have escaped.

Action provides a comprehensive, easy-to-use solution. For example, if a user attempts to copy a critical file, **Action** sends an SMS message to the security officer's mobile phone and automatically signs off and disables the offending user. Scripts can even initiate actions that take place if an appropriate response does not occur within a specified period of time! **Action** real-time detection constantly monitors the system for a wide variety of security and other system events, including:

- > Events detected by **Audit** real-time auditing
- > Transactions detected by **Firewall** network security rules
- > Terminal screens locked/released and jobs terminated by **Screen**
- > Active job status and checking for jobs that are not active
- > Current system and memory pool status



Action Real-Time Detection rule process

It is amazingly easy to define rules and actions with the 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 operators such as: equal/not equal, greater than /less than, like/not like, "contained in list", "Starts with", etc. No other security alert/action system offers such power and flexibility.

Action also includes a number of other 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.



IBM Server

Type choices, press Enter.

Action Name OBJCHANGE
Description. Object Change

Define alert message recipients

1=E-mail 2=Message Queue 3=User 4=Remote User 5=LAN user 6=SMS 7=Special

Message ID *AUTO *AUTO, Message ID

Type Recipient address, *USER, *DEV, *JOB, *SYSTEM

1 ADMIN@RAZLEE.COM

2 QSECOFR

6 888-729-5332

More...

F3=Exit F4=Prompt

F12=Cancel

Terminal window screenshot showing the configuration steps for adding an alert message, including action name, recipients, and message ID.

Send alert messages to security personnel by SMS, pager, email, etc.

U.S. Office & Corporate HQ

12 Englewood Ave Nanuet, New York 10954
Toll Free Tel: 1-888-RAZLEE-4
Fax: 1-419-781-5851

Research & Development

71 Hanadiv St. Hertzliya, Israel 46485
Tel: +972-9-9588860
Fax: +972-9-9588861

E-mail: info@razlee.com

www.razlee.com