Action

DATASHEET (iSecurity Suite Auditing & Monitoring)

Automated Security Breach Reporting and Corrections

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.

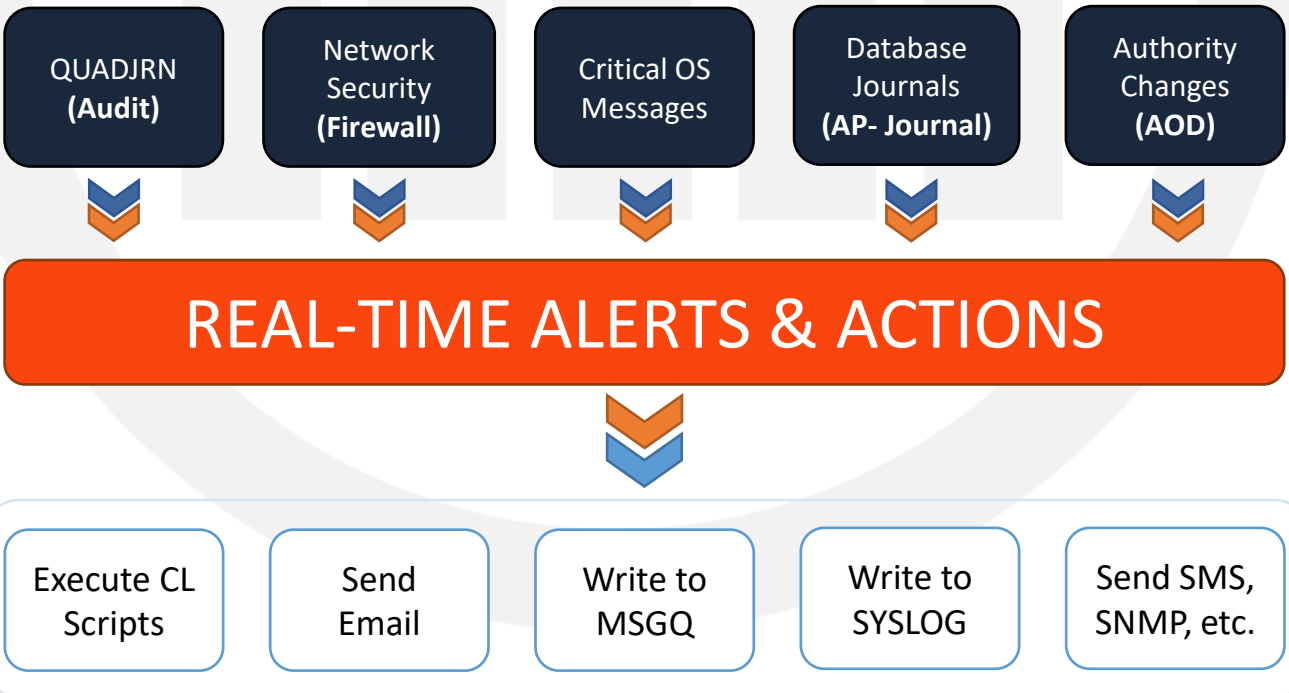
Take in Charge with iSecurity Action

iSecurity Action provides a comprehensive, easy-to-use solution. For example, if a user attempts to copy a critical file, Actions 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 Workflow

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



Key Features

- 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 events detected by Audit, Firewall, AP-Journal, Anti-Virus, Authority on Demand, etc.
- 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

iSecurity Action Benefits

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.

Action real-time detection continuously 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
- 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

Let’s Get Started

Schedule your Demo and start Auditing & Monitoring your Systems with iSecurity Action.

RAZ-LEE iSecurity