ACTION

Automated Security Breach Reporting and Corrections

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

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

ACTION

Automated Security Breach Reporting and Corrections

RAZ-LEE iSecurity

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 Actions 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!

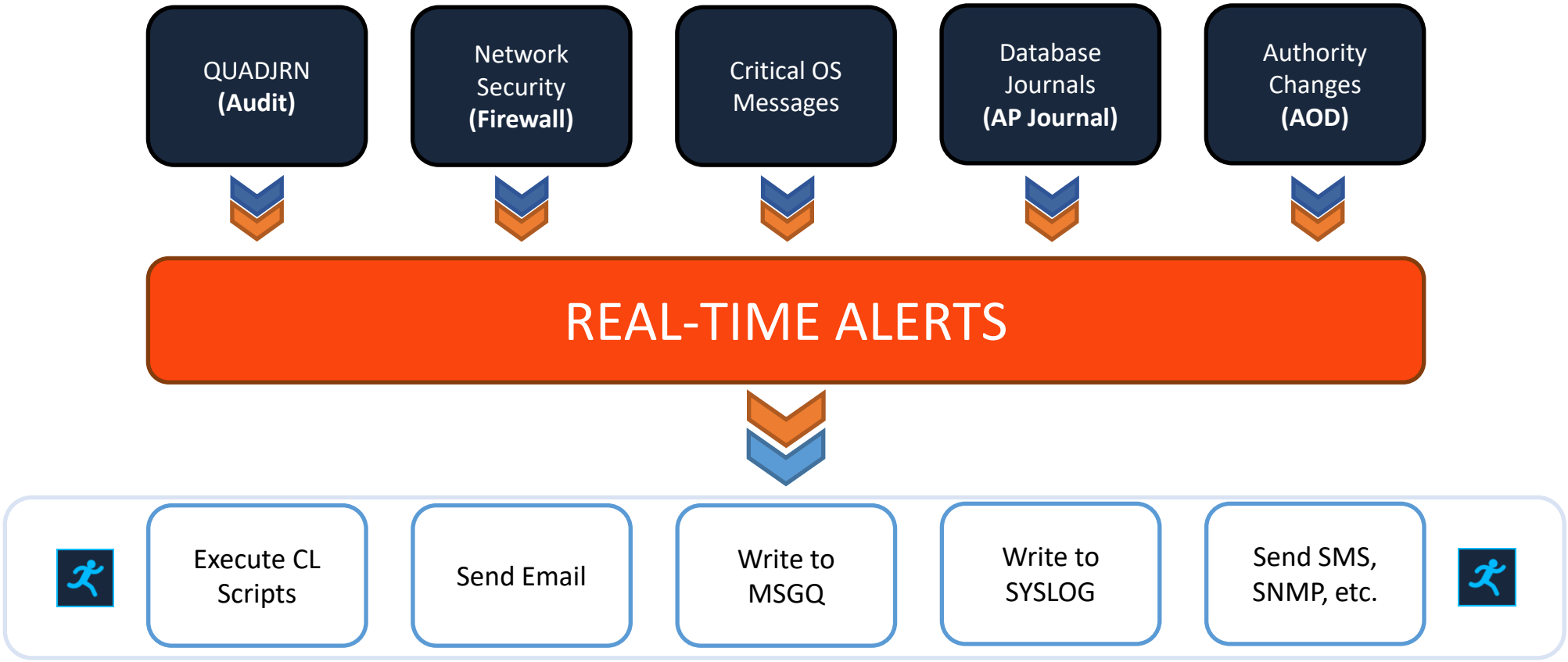
Real-time Detection

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 Anti-Virus
- Suspicious data changes by AP-Journal
- Active job status and checking for jobs that are not active
- Current system and memory pool status

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

- 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, Antivirus, 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

Thank You

For more information about our company and products please visit

www.razlee.com