COMMAND

Command-line Control & Monitoring

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

imperva IBM McAfee

Akamai RSA SEA SOFTWARE ENGINEERING OF AMERICA

RAZ-LEE iSecurity

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

COMMAND

Command-line Control & Monitoring

RAZ-LEE iSecurity

Risk at the Command-line

Command-line (CL) commands control nearly all IBM i functionality. As such, monitoring, controlling and logging CL commands is essential for both the ongoing functioning of the company and compliance with regulations such as GDPR, SOX, HIPAA, PCI and auditor-mandated policies.

- A minor change in a CL command parameter can cause severe damage, yet it is difficult to control the use of CL commands and their parameters.

- Unauthorized and uncontrolled use of CL commands and their parameters pose a major corporate risk. Companies and their auditors require greater control of CL commands.

Total Control Over CL Commands

iSecurity Command provides total control over system & user defined CL commands, regardless of how the CL command was entered.

Provides the ability to control CL commands, their parameters, origin, context (i.e. the program which initiated the CL command), the user issuing the CL command, etc., and provides easy-to-define ways to react to these situations.

- Allow normal CL command processing
- Allow CL command processing after modifying parameters or parts of parameters
- Execute a different CL command
- Reject the CL command

Support for Complex Parameter Structures

Unique Support for Complex Parameter Structures. The structure of CL command parameters can be complex; for example, some of the Change User Profile (CHGUSRPRF) parameters are:

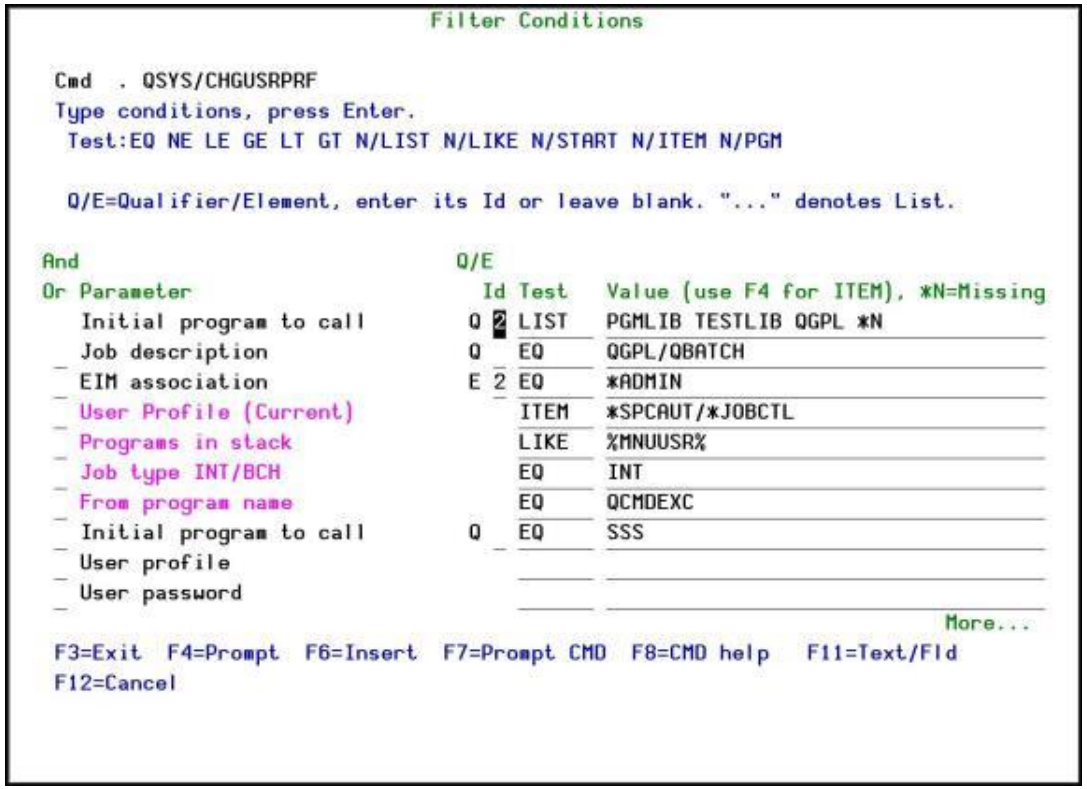
- Qualified such as: INLPGM(library / program)
- Composed of elements such as: EIMASSOC(admin *ADMIN *REPLACE)
- Include a list of values such as: SUPGRPPRF(grpprf1 grpprf2 gprpprf3)

To properly analyze a CL command parameter, accurate referral is required. Command is the only product that has the ability to refer, for analysis or change, to each part of a complex parameter separately, as well as to the parameter as a whole.

Command includes a variety of selection criteria which enable replacing, adding or removing qualifiers, elements and list elements!

Filter Conditions

Filter conditions are the criteria that must be matched when a command is entered by a user in order to trigger the command's alerts, messages and changes. Each filter condition consists of a comparison test applied against one of the fields in the journal record, such as a parameter, originator (job, user, IP) or context (from which program, environment).



RAZ-LEE iSecurity

Log and Event Manager

When a command rule is matched, a message can be generated to alert different users.

- CL command Reject or Allow with or without modifications may initiate alerts by e-mail, Syslog or SIEM.
- Replace, prior to execution, an element, a qualifier, an entire parameter or the CL command itself
- Extensive log with a full Report Generator produces HTML and PDF reports and sends them by e mail

iSecurity Command Advantages

- System or User Defined CL commands can be filtered according to the relationship between parameters, originator (job, user, IP) and context (from which program, environment)
- Reference to a specific qualifier or element allows differentiating between “PAYROLL” as part of the file or library name itself
- Selection criteria include EQ, LIST, LIKE, START, etc. and ITEM, which ensures the existence of a specific user in an external table to verify that the user has, for example, special authority

Thank You

For more information about our company and products please visit

www.razlee.com