Command

DATASHEET (iSecurity Suite Network Protection)

Command-line Control & Monitoring

CL commands control nearly all IBM i functionality. As such, monitoring, controlling and logging CL commands is essential for both the on-going functioning of the company as well as to comply with regulations such as 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.

CL commands are entered in different ways: from the CL command line, by selecting an option from a menu, as part of a program, via FTP and more.

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

Our Solution

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

Reacting to CL Commands

During CL command processing, iSecurity Command is able to:

- 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

And, as iSecurity Command is totally integrated into the infrastructure of products in the iSecurity Suite, it can send real-time alerts as event-specific e-mails or SMS, Syslog and other forms of messages. Command can even trigger the execution of a CL script.

Key Features

- 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 name or the 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
- CL command Reject or Allow with or without modifications may initiate alerts by e-mail, Syslog, etc.
- 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
- Command has been designed and implemented based upon specific customer requests for a “total” control and monitoring solution.

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:

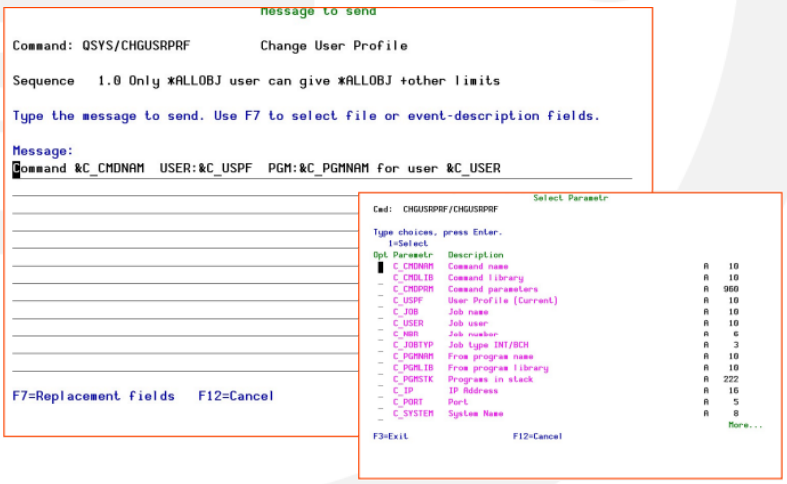
- Qualified such as: INLPGM(library / program)
- Composed of elements such as: EIMASSOC(admin *ADMIN *REPLACE)
- Include a list of values such as: SUPGRPPRF(grpprf1 grpprf2 gprpprf3)

To properly analyze a CL command parameter, accurate referral is required. iSecurity 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.

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

Real Time Alerts

Sends real-time alerts as event-specific e-mails or SMS, Syslog, MSGQ messages. iSecurity Command Can even execute CL script.



Let’s Get Started

Schedule your Demo and start using Network Protection on your Systems with iSecurity Command.

RAZ-LEE iSecurity