Capture

Visual Track for System i Green-Screen User Activity

In today's increasingly complex business environment, effective and searchable audit trails are a key component of any organizational IT security program.

IT departments and technical support personnel need to monitor user activity in order to troubleshoot error conditions, track performance bottlenecks, and ensure compliance with organizational policies. This often requires detailed knowledge of what users are doing and how they are doing it.

Any Way to have a Visual Track?

iSecurity Capture solves this problem by complementing journals and reports with a visual audit trail of user activity.

- Capture shows exactly what users are doing and when they are doing it! Screen capture sessions are initiated as required and are retrievable using an intuitive process featuring flexible scrolling and a powerful free-text search engine for locating the captured data screens and logs.

- Within each screen capture session, you can scroll through the screens sequentially or you can use the moveable Capture Menu to jump directly to a particular screen or search for screens containing a specific text string.

Our Solution

iSecurity Capture solves this problem by complementing journals and reports with a visual audit Capture is a green-screen tracking solution that automatically captures and saves user activity as displayed on System i (AS/400) screens. Capture's invaluable tracing capabilities allow organizations to conform with compliance requirements that apply to industries such as banking, insurance, health care, and defense.

- Runs either in "silent-mode" or as a deterrent known to possible offenders

- Automatically triggers screen capturing according to a variety of pre-defined rules

- Searches screens for suspicious content using a powerful text search capability

- Saves hours of tedious work and costly phone calls in the event of an application-related problem

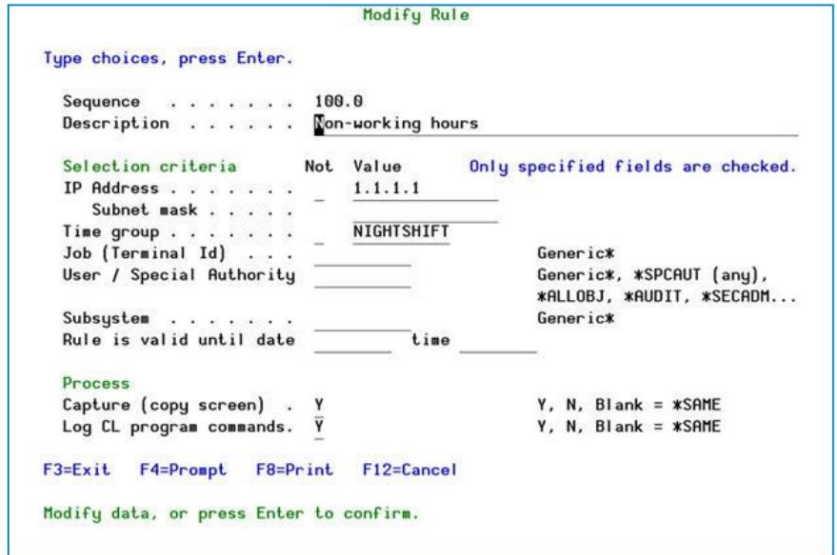- Retrieves captured user screens easily via a user-friendly display

Key Features

- Preserves job logs and CL Command logs for subsequent review, even after a session is finished
- Uses a simple rule definition process suitable for both IT professionals and non-technical users
- Archives captured screens offline to meet data retention requirements without consuming excessive disk resources
- Searches user sessions in a specific timeframe, in accordance with any screen content, for example, mortgage or patient number specified in the screen
- Easy navigation through captured sessions via moveable Capture Menu

iSecurity Capture Capabilities

The Capture Menu also provides commands for displaying the job log and the Audit log entries related to the particular screen and capture session.

You can even access the DSPJOB command and print the screen directly from the Capture Menu.


```
                              Modify Rule

Type choices, press Enter.

    Sequence  . . . . . . .   100.0
    Description  . . . . . .   Non-working hours

    Selection criteria        Not  Value        Only specified fields are checked.
    IP Address . . . . . . .    _   1.1.1.1
        Subnet mask . . . . .
    Time group . . . . . . .    _   NIGHTSHIFT
    Job (Terminal Id)  . . .                     Generic*
    User / Special Authority                     Generic*, *SPCAUT (any),
                                                 *ALLOBJ, *AUDIT, *SECADM...
    Subsystem  . . . . . . .                     Generic*
    Rule is valid until date           time

    Process
    Capture (copy screen)  .   Y                 Y, N, Blank = *SAME
    Log CL program commands.   Y                 Y, N, Blank = *SAME

F3=Exit   F4=Prompt   F8=Print   F12=Cancel

Modify data, or press Enter to confirm.
```

Capture works both a stand-alone product and also as a module fully integrated into the iSecurity Suite.

Let's Get Started

Schedule your Demo and Keep Visual Track with iSecurity Capture

RAZ-LEE iSecurity