

# [ Beta 89 zSecurity Monitor ]



## Monitoração Automatizada do RACF

### Escalonamento imediato de eventos de segurança

O Beta 89 zSecurity Monitor é um software de monitoração de segurança para garantir a proteção do z/OS em tempo real. O módulo utiliza a rotina SMF-Exit desenvolvida pela Beta Systems para a monitoração das atividades do RACF e escalona automaticamente os eventos de segurança para seus destinatários. Isto permite uma análise automática de registros SMF para eventos de violação de segurança.

### Reação rápida aos eventos de segurança

Em caso de ataques dirigidos, mas também em eventos originados por erros de usuário, a rápida reação ao evento é o fator decisivo, pois extensos prejuízos podem ocorrer. O Beta 89 zSecurity Monitor possibilita ao pessoal da segurança de TI uma reação imediata diante de eventos de segurança.

### Vantagem de tempo para auditoria e administração

O Beta 89 zSecurity Monitor é uma ferramenta que economiza tempo na execução de tarefas de auditoria e administração. Cria relatórios que correspondem precisamente aos seus requisitos e são adequados para determinados eventos.

### Escalonamento imediato

O Beta 89 zSecurity Monitor informa sobre eventos de segurança imediatamente, por exemplo, via e-mail, NT, console do sistema ou TSO SEND e pode notificar sistemas de monitoração existentes como o Tivoli, entre outros. Todos os eventos notificados são protocolados para auditoria. O escalonamento em grupos de console NT pode ser dividido conforme as áreas de responsabilidade.

### O que você ganha com a utilização do Beta 89 zSecurity Monitor

- Elevação dos padrões de segurança através de monitoração automatizada.
- Suporta a administração de segurança.
- Economia de tempo pelo imediato escalonamento.
- Tempo de reação melhorado devido à identificação direta do evento.
- Identificação imediata de eventos relevantes à segurança.
- Vantagem de tempo através do escalonamento imediato via e-mail, console NT, console do sistema e console Tivoli.



## Exemplos de eventos de segurança

- Alterações no ambiente RACF.
- Alterações nas definições de verificação.
- Acesso aos recursos z/OS.
- Manipulação direta do banco de dados.
- Acesso a dados protegidos.
- Alterações nos conjuntos de dados do sistema operacional.
- Login no sistema z/OS.
- Logins feitos por usuários desconhecidos.
- Alterações repetidas de senha durante o login.



## Segurança através da análise automatizada de dados SMF

Antes que o Beta 89 zSecurity Monitor aplique o filtro e as regras de notificação para um evento de segurança, a informação do evento é padronizada através da sua conversão para um registro de evento padrão (SER – Standard Event Record).

## Registro de evento padrão

O registro de evento padrão contém as seguintes cinco características básicas de um evento:

- Quem é responsável pelo evento?
- Qual evento ocorreu?
- Onde ocorreu o evento?
- Quando ocorreu o evento?
- Qual foi o efeito do evento?

## Filtragem de dados

O Beta 89 zSecurity Monitor monitora conjuntos de dados SMF designados para o RACF. Através da análise automática de registros SMF relativos a violações de segurança, os eventos relevantes podem ser identificados e escalonados imediatamente. Os procedimentos de filtragem e análise podem ser alterados sem a reinicialização do sistema.

## Logging (Registro dos Eventos)

Cada evento notificado é registrado para fins de auditoria. O protocolo ativo pode ser solicitado on-line a partir de interfaces TSO e gráfica.

## Configurações predefinidas do sistema

O Beta 89 zSecurity Monitor está equipado com um conjunto básico de filtros e regras de ação, os quais possibilitam um início imediato da monitoração de segurança.



A GFS Software é distribuidora dos Produtos da Beta Systems no Brasil.

**GFS**  
SOFTWARE

**GFS Software e Consultoria Ltda.**  
São Paulo | Brasília | New York

E-mail: gfs@gfs.com.br  
www.gfs.com.br