Enforcive™
Data respected.

Workers
INFORMÁTICA

Enforcive Enterprise Security
CPA para Mainframe

MONITOR DE DADOS CRÍTICOS DO MAINFRAME PARA EVENTOS DE SEGURANÇA E DE SISTEMA VIA INTERFACE GRÁFICA.

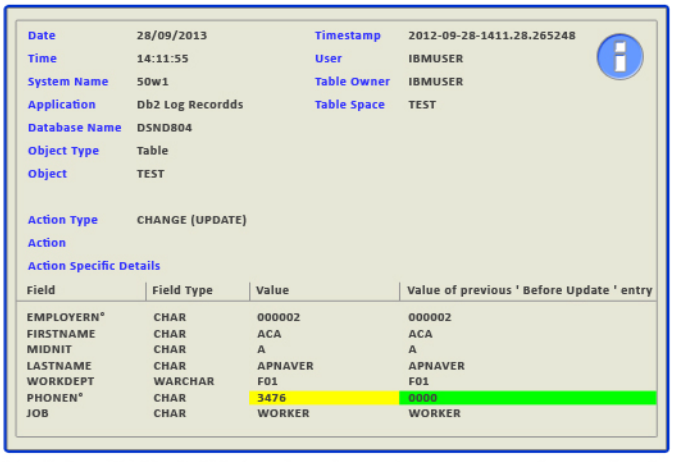

GRÁFICOS


ALERTAS, E-MAIL


LOGS DE AUDITORIA


SYSLOG

- SMF TELNET
- SMF RACF
- SMF FTP
- TCP/IP FTP / Telnet
- SMF VSAM
- SMF DB2
- Dados DB2 Antes / Depois
- Enforcive/CICS



Registro DB2 – Exibição de valores de campos antes e depois

GERADOR DE RELATÓRIOS

Tem a capacidade de exportar relatórios para o MS Excel, PDF e outros formatos. A geração de relatórios pode ser agendada periodicamente, com frequência diária, semanal ou mensal.

EXIBIÇÃO FÁCIL E CLARA DA AUDITORIA DE SEGURANÇA

Trilha de auditoria intuitiva e amigável de eventos de SMF e de outros dados de auditoria produzidos por DB2, RACF, FTP e atividade Telnet. Os eventos são decompostos em função dos parâmetros definidos, facilitando sua compreensão.

Workers Informática | E-mail: info@workers.com.br • Site: www.workers.com.br

CRITÉRIOS DE FILTRAGEM DETALHADA PARA ANÁLISE DE EVENTOS DE SEGURANÇA

O auditor de segurança pode visualizar eventos de segurança on-line e filtrá-los na tela, sem a necessidade de aplicativo ou programação adicional. A filtragem pode ser realizada por: data e hora, plataforma, tipo de conta, usuário, status do evento, endereço IP e tipo de evento da aplicação.

Os eventos podem ser filtrados por aplicação: log do DB2, SMF RACF, SMF DB2, auditoria de aplicação TCP/IP , SMF telnet, SMF FTP, Enforcive/Security for CICS.

Adicionalmente, os eventos podem ser filtrados por aplicação, categoria, tipo e sub-tipo de evento. Como exemplos, podemos citar:

- Log do DB2 > tabela de alterações auditadas > exclusão/inserção/atualização
- SMF DB2 > falhas de autorização > privilégios de database > exibição de database

GRÁFICOS DINÂMICOS

Gráficos podem ser gerados para observar tendências e identificar o comportamento da atividade do sistema. O usuário pode navegar a partir do ponto inicial escolhido até atingir a seleção desejada. Os gráficos podem ser impressos, armazenadosno PC ou enviados por e-mail. Eventos oriundos de toda a empresa podem ser combinados, classificados e filtrados, gerando centenas de combinações diferentes por plataforma, aplicação, endereço IP, usuário, status e data da transação. Os gráficos são criados dinamicamente pelo usuário, selecionando o parâmetro de classificação em cada nível.

Cada componente dos gráficos exibidos podem ser expandidos com o click do mouse para mostrar os eventos de auditoria atuais usados para gerar as estatísticas e cada evento pode ser detalhado para mostrar todas as informações relacionadas, incluindo o nome e o valor de cada parâmetro de evento.

Os gráficos incluem visões estatísticas e ao longo do tempo dos eventos de auditoria. Os gráficos e os sumários podem ser exibidos na tela, impressos, enviados por e-mail e armazenados em vários formatos, incluindo PDF e HTML compatível com o MS Office.

EXPORTAÇÃO DOS DADOS DE AUDITORIA DO MAINFRAME PARA O PC

Após a transferência dos dados de auditoria do mainframe para um banco de dados em um servidor MS SQL, os arquivos de log originais podem ser deletados do sistema, liberando assim um valioso espaço em disco. Uma vez importados para o CPA (Cross-Platform Audit), as informações podem ser visualizadas e analisadas a partir de um PC. As transferências podem ser agendadas para ocorrerem automaticamente.

Enforcive™
Data respected.

Workers
INFORMÁTICA

CONSOLIDAÇÃO DE DADOS DE SEGURANÇA DE MÚLTIPLOS SISTEMAS

Os dados de auditoria de segurança provenientes de qualquer número de mainframes, bem como de IBM i, MS Windows, MS SQL Server, Linux, AIX, Oracle e outros podem ser consolidados em um único local. A importação de dados de auditoria de outros sistemas requer a instalação de agentes Enforcive nos mesmos. Usuários lógicos, chamados de usuários IDS, podem ser criados para auditar a atividade de um usuário com diferentes identificações de logon. O usuário IDS não requer uma identidade pré-definida como no caso da implementação de sign-on único.

PLATAFORMAS SUPORTADAS

- IBM iSeries
- Windows
- Unix / AIX
- Oracle
- SAP
- IBM Mainframe (Z)
- SQL Server
- Linux
- AIX / DB2