SF-SHERLOCK®

SEU OBJECTIVO

MÁXIMA SEGURANÇA

MÁXIMA QUALIDADE

NA Z PLATAFORMA ATRAVÉS

DE AUTOMATIZAÇÃO

COM O MÍNIMO DE ESFORÇO

PROTECÇÃO TÉCNICA E LEGAL

ATRAVÉS DE UM CONTROLO

DETALHADO E COMPLETO

EM TEMPO REAL

» UMA DA INOVAÇÕES MAIS FUNDAMENTAIS NO SECTOR DA SEGURANÇA DE MAINFRAME DESDE O RACF. «

CONTROLO TOTAL DE SEGURANÇA E QUALIDADE NA Z-PLATAFORMA

Você está consciente dos riscos e perigos que existem hoje em dia e por isso dá o máximo valor à segurança informática para proteger o capital da sua empresa. Na Era da Internet e do Comércio Electrónico você quer continuar a confiar na ideia »mainframe = segurança máxima«.

Você conhece as actuais e rigorosas normas e recomendações legais como Basel II, o manual de »Protecção fundamental nas Tecnologias de Informação« (Ministério Alemão de Segurança das Tecnologias de Informação), Sarbanes Oxley (SOX), U.S. DOD Regulations, Gramm Leach Bliley Act (GLBA), KonTraG, RS FAIT 1, HIPAA Security, 95/46/EC, Data Protection Directive , etc. e os critérios de **certificação segundo ISO ou BS**. Estes estandartes exigem da sua empresa a aplicação de medidas precisas, eficazes e efectivas para assegurar todos os processos baseados na tecnologia de informação e sua auditoria correspondente, incluindo a tecnologia subjacente contra ataques internos e externos. **Ademais, também precisa de provas claras para os seus clientes, accionistas e legisladores** que comprovam que todo o possível foi feito tanto tecnica como legalmente para garantir o máximo nível de segurança e qualidade, e também para conseguir uma boa avaliação [de riscos]. O seu objectivo para o mainframe da sua empresa é cumprir todas essas exigências legais e técnicas com o mínimo de esforço. E é por isso que você procura uma solução detalhada e completa com auditoria, que trabalhe automaticamente e tecnicamente com a máxima eficiência e que seja legalmente aceitada.

Você considera a segurança, a qualidade e a eficiência de custos como factores de competitividade altamente importantes. Você sabe que somente com a máxima qualidade e o máximo nível de automatização nos processos de trabalho diário pode conseguir a maior produtividade exigida, criando assim a flexibilidade e o tempo necessário para enfrentar as actuais mudanças empresariais e as futuras oportunidades.

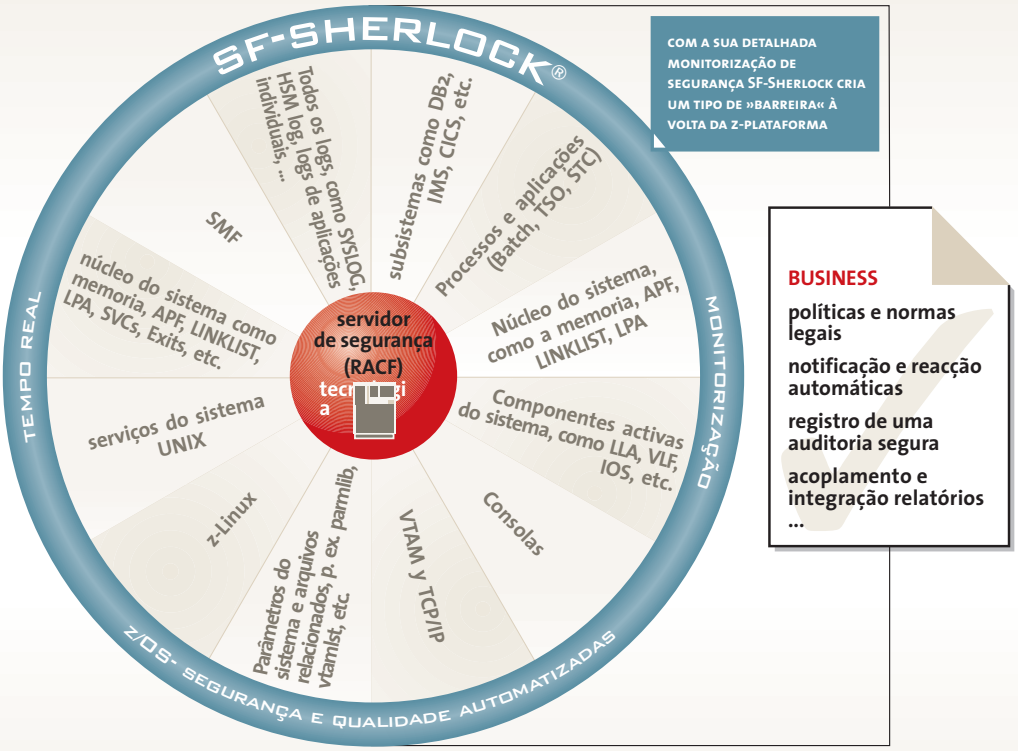
Você quer uma solução única que realize todas as tarefas necessárias, como o controlo de incidentes, análises dos pontos fracos do seu sistema através de uma avaliação permanente de vulnerabilidade e praticamente cobrindo **todo o sector técnico da plataforma mainframe**. Ao mesmo tempo, esta solução deveria permitir uma aplicação diária e uma cooperação organizada entre **todos os departamentos, do nível técnico até ao mais alto nível de gestão**.

Ademais, você exige a possibilidade de integração na gestão de segurança da empresa inteira e das soluções de auditoria. Você nunca quer duvidar dos seus investimentos nesta área. A solução que você exige deve apoiar sistematicamente seus interesses, também dentro do marco de **ITIL, COBIT, BS7799**, entre outros.

Z SEGURANÇA E QUALIDADE AUTOMATIZADAS COM SF-SHERLOCK É A RESPOSTA AOS NOVOS CAMPOS DE Z- APLICAÇÕES NA ERA DA INTERNET E DO COMÉRCIO ELECTRÓNICO

PERFORMANCE

- PROTECÇÃO DE 24 HORAS ATRAVÉS DE UM CONTROLO EM TEMPO REAL
- MONITORIZAÇÃO DE APLICAÇÕES
- REDUÇÃO DE TRABALHO E CUSTOS
- GARANTIA TOTAL DE QUALIDADE
- DETECÇÃO DE ABUSOS DE AUTORIZAÇÃO E MANIPULAÇÕES (DINÂMICAS) DAS FUNÇÕES DE PROTOCOLO E DE REGISTRO, DA MEMORIA,...
- DETECÇÃO DE ACTIVIDADES SUSPEITAS E DE EXTRUSÃO VIA AS CHAMADAS TRAMPAS LÓGICAS
- NOTIFICAÇÃO E REACÇÃO AUTOMÁTICA
- REVISÃO DE AUDITORIA E INTEGRAÇÃO
- MONITORIZAÇÃO DE FICHEIROS COM DELTA REPORTING
- MONITORIZAÇÃO DE INTRUSOS E USUÁRIOS INTERNOS
- DETECÇÃO DE INTRUSÃO E EXTRUSÃO
- CUMPRIMENTO DE NORMAS LEGAIS COMO SOX, KONTRAG, ISO, BS, US, DOD, MINISTÉRIO ALEMÃO DE SEGURANÇA
- MÁXIMO SUPORTE PARA TODOS OS DEPARTAMENTOS
- RELATÓRIOS INCLUINDO PONTUAÇÕES
- POSSIBILIDADE DE ACOPLAR-SE A SISTEMAS DE TICKET, DE PROBLEMAS OU OUTROS ITIL-SISTEMAS
- RELATÓRIOS ESPECÍFICOS PARA CADA CLIENTE
- PROTECÇÃO E DEFESA CONTRA USO INDEVIDO
- INTERFACES ABERTAS PARA UMA INTEGRAÇÃO FÁCIL
- ANALISES PERMANENTE DE PONTOS FRACOS COM UMA PENETRAÇÃO SUAVE SEM POSSÍVEIS INTERFERÊNCIAS
- TESTE DE QUALIDADE DE CONTRA-SENHAS
- CAPAS DE APLICAÇÃO COMO MEDIDA CONTRA ATAQUES COMO BUFFER OVERFLOW, FORMATO STRING, ETC
- SUPORTE PARA TODO O TIPO DE FONTE, COMO SMF, LOGS, ...
- POLITICAS EXTENSAS RESULTADOS SEGUROS DE AUDITORIA (LOGS, RELATORIOS, ETC.)
- SIMULAÇÃO (IPL)
- ANALISE SINTÁCTICA E SEMÂNTICA DE ARQUIVOS DO SISTEMA, COMO PARMLIB, VTAM 1 ST, ECT.
- FUNCIONAMENTO TOTALMENTE AUTOMATIZADO
- KITS DE CONEXÃO PARA A INTEGRAÇÃO FÁCIL NA SEGURANÇA DE MÚLTIPLAS PLATAFORMAS E SOLUÇÕES DE GESTÃO DO SISTEMA, COMO SYMANTEC, CA, TIVOLI, ETC.



A SOLUÇÃO : SF-SHERLOCK MONITORIZAÇÃO EM TEMPO REAL

»Tecnologia:___SF-Sherlock representa a tecnologia de alta performance de **monitorização em tempo real para estabelecer uma automatização completa de segurança e qualidade** na z-plataforma integrando o controlo, a gravação, o relatório e as possibilidades de simulação (p. ex. IPL) em uma solução única. Com as suas componentes, SF-Sherlock é um processo permanente dentro do sistema que controla e examina o sistema de segurança (tanto o servidor de segurança ou RACF como também CA-TopSecret e CA-ACF2), processos específicos e subsistemas (DB2, LDAP, etc.) e também o sistema operativo z/OS e todas as suas componentes. SF-Sherlock grava alterações relevantes de maneira segura e informa a pessoa responsável a tempo e especificamente sobre os incidentes relacionados com o seu sector, como erros, ataques, manipulações, alterações, etc., por exemplo via e-mail ou SMS. Desta maneira, o departamento de auditoria consegue um controlo e uma avaliação automatizados, incluindo relatórios. Isto significa que ninguém tem que proceder manualmente os resultados e ninguém perde tempo com tarefas rotineiras porque todos os processos estão completamente automatizados. **Este método dá-lhe liberdade, flexibilidade e segurança**. Em determinados casos, SF-Sherlock ainda vai mais longe de simples relatórios. Por exemplo, com as sua facultativa reacção automática e instantânea, SF-Sherlock remove intrusos imediatamente do sistema. Com este controlo e esta observação permanentes no sentido de uma **protecção de 24 horas**, você consegue o máximo nível de segurança e qualidade. E deste modo, você domina o seu sistema e reduz os custos.

»A necessidade de agir é indiscutível:___Desde 2004, o Ministério Alemão de Segurança Informática (BSI) – com o seu Manual de Segurança »Protecção fundamental nas Tecnologias de informação« – vai ainda muito mais longe que as normas do Ministério de Defesa dos Estados Unidos, analisando abertamente os riscos e definido as medidas de segurança necessárias para a plataforma do z/OS mainframe. A mensagem principal descreve **a exigência de »utilizar uma monitorização de segurança em tempo real de sistemas z/OS para poder determinar mais rapidamente violações de segurança«**. Uma monitorização em tempo real de um único aspecto de segurança, como os protocolos SMF, é simplesmente insuficiente. É preciso uma monitorização do z/OS inteiro com todas as suas componentes e com todas as relações e detalhes complexos. SF-Sherlock controla o sistema de z/OS detalhada e completamente, já que o maior perigo vem através de processos difíceis que passam desapercebidos e erros ocultos em qualquer lugar dentro do z/OS, como p.ex. conseguir uma autorização mais elevada, romper o processo de auditoria ou obter acesso desapercebido a recursos. Desta maneira, especialistas podem espiar todos os dados evitando e manipulando o sistema de segurança sem deixar rastro de um único protocolo no SMF ou no registro. Correspondentemente, parâmetros e configurações errados do sistema que passam desapercebidos podem por em perigo a disponibilidade de todo o sistema, pelo menos até à próxima IPL. Tanto défices na segurança como na qualidade representam uma catástrofe e têm que ser evitados »a todos custos«. Por isso, depois de cada modificação dentro do sistema, **SF-Sherlock analisa automaticamente o seu sistema de segurança tanto como o seu parmlib e outros arquivos importantes a procura de erros possíveis**. Uma tecnologia em tempo real é necessária porque o tempo de vida de manipulações das actividades ilegais profissionais é extremamente curta – detecção, prevenção através de reacção e uma constante apresentação de provas não são possíveis de outra maneira. A lista de possíveis vulnerabilidades e erros é muito larga e só pode ser cumprida com um controlo totalmente automatizado.

»Tecnologia que garante sucesso:___A tecnologia automática e completa para a garantia de segurança e qualidade de SF-Sherlock apoia completamente os objectivos aqui mencionados e faz com que a sua plataforma de mainframe cumpra todas as normas legais. Com SF-Sherlock você não só encontra os requisitos necessários como também consegue uma **garantia total de qualidade e uma protecção completa**. SF-Sherlock prepara um caminho seguro para o futuro da sua empresa. O controlo e a analise constantes e completos, especialmente a níveis técnicos mais profundos, é cada vez mais importante com as novas funções do z/OS (Unix/USS, Sysplex, etc.) e as novas áreas de aplicação como servidores de rede, servidores de dados e plataformas de comercio electrónico. Não há duvidas de que assim as medidas estandartes cada vez parecem mais insuficientes. A função de **SF-Sherlock como sistema de detecção de intrusão e extrusão para a defesa contra ataques internos e externos** é ainda mais importante na sua função como nível mais alto de protecção contra a crescente abertura de sistemas e redes que até agora estavam fechados. Com a sua tecnologia líder, SF-Sherlock é um passo essencial para chegar a um nível de segurança e qualidade constante e actual para combater estes riscos.

»Produtividade que garante sucesso:___Como processo automático em tempo real, SF-Sherlock trabalha tanto para os departamentos de segurança, auditoria, protecção de dados e informação como para o departamento de tecnologia do sistema. E ainda mais, SF-Sherlock integra os num processo comum e altamente eficiente que leva a **uma produtividade mais elevada e uma redução de gastos importante**. Pela sua automatização completa de segurança e qualidade, SF-Sherlock é uma solução integrada para toda a empresa, também na área de plataformas múltiplas. O seu valor acrescentado garante a mais alta rentabilidade e eficiência de custos para todos os que estão envolvidos. Com o conceito de implementação Plug&Play, você atingirá esse objectivo, terá menos trabalho e cumprirá as normas legais com o mínimo em tempo, custos e esforços.

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM