SF-SHERLOCK®

VOS OBJECTIFS

LA PLUS HAUTE SÉCURITÉ

LA PLUS GRANDE QUALITÉ

SUR LA PLATE-FORME Z

PAR AUTOMATISATION AVEC

UN MINIMUM D'EFFORTS

PROTECTION TECHNIQUE ET

ASSURANCE D'UNE

CONFORMITÉ LÉGALE

PAR UNE SURVEILLANCE

COMPLÈTE EN TEMPS RÉEL

» L'UNE DES INNOVATIONS LES PLUS ESSENTIELLES DANS LE DOMAINE DE LA SÉCURITÉ MAINFRAME DEPUIS RACF. «

SURVEILLANCE TOTALE DE LA SÉCURITÉ ET DE LA QUALITÉ POUR LA PLATE-FORME Z

Vous êtes conscient des risques d'aujourd'hui et attachez donc la plus haute importance à la sécurité informatique pour protéger la fortune de votre entreprise. A l'ère d'Internet et du commerce électronique, vous souhaitez pouvoir continuer à vous fier à l'idée: «mainframe = sécurité maximale».

Vous connaissez la rigueur de la réglementation et des recommandations actuelles comme Basel II, le manuel de protection informatique (bureau allemand pour la sécurité informatique), Sarbanes Oxley (SOX), Gramm Leach Bliley Act (GLBA), KonTraG, RS FAIT 1, HIPAA Security, direction de protection des données 95/46/EC, etc. et les critères de certifications ISO ou BS. Ces standards exigent de votre entreprise des mesures précises, efficaces et effectives pour sécuriser tous les processus informatiques incluant une technologie poussée contre les attaques provenant de l'intérieur et de l'extérieur. **Vous avez donc besoin d'une preuve évidente des bénéfices apportée aux client, aux actionnaires et aux législateurs** en démontrant que tout ce qui est possible, aussi bien techniquement que légalement, a été fait afin de garantir les plus hauts standards de sécurité et de qualité – également pour atteindre **une bonne estimation [des risques]**. L'objectif pour le système centralisé (mainframe) de votre entreprise est de correspondre à toutes ces exigences légales et techniques avec un minimum d'efforts. Vous recherchez donc une solution pratique, automatique, hautement efficace d'un point de vue technique et légal et sécurisée concernant l'audit.

Vous considérez la sécurité, la qualité et la réduction des coûts comme des facteurs de compétitivité de la plus haute importance. Vous savez que vous ne pouvez atteindre la plus grande productivité qu'avec une qualité irréprochable et le plus haut niveau d'automatisation dans les processus du travail quotidien. Ceux-ci vous donneront la flexibilité et le temps nécessaires pour vous adapter aux «véritables» exigences des entreprises, d'aujourd'hui et de demain.

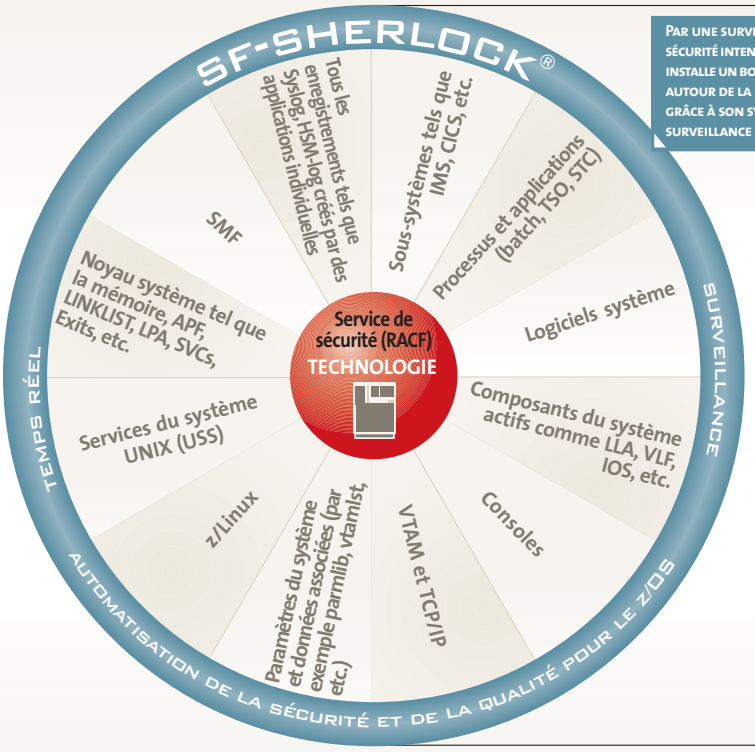
Vous souhaitez une solution unique qui vous permette d'effectuer toutes les tâches nécessaires, telles que la surveillance constante d'événements et l'analyse des points faibles de votre système et recouvrant **totalement l'éventail technologique de la plate-forme (mainframe)**. Cette solution vous permettra en même temps une utilisation quotidienne et l'organisation du travail en coopération, correspondant à votre niveau de créativité, de tous les départements, **de la sphère technique au plus haut niveau de direction**.

Vous exigez également l'ouverture à l'intégration dans la gestion de la sécurité de votre plate-forme et aux solutions d'audit dans le cadre de votre entreprise. Vous ne souhaitez pas remettre vos investissements en question dans ces domaines, mais voulez être assuré que vos intérêts seront soutenus, également comme par exemple dans le cadre de **ITIL, COBIT, BS7799**, entre autres.

L'AUTOMATISATION DE LA SÉCURITÉ Z ET DE LA QUALITÉ AVEC SF-SHERLOCK EST LA RÉPONSE AUX NOUVEAUX CHAMPS D'APPLICATION Z À L'ÈRE D'INTERNET ET DU COMMERCE ÉLECTRONIQUE

PERFORMANCES

- PROTECTION 24 HEURES SUR 24 PAR UNE SURVEILLANCE EN TEMPS RÉEL
- SURVEILLANCE DES APPLICATIONS
- ALLÈGEMENT DU TRAVAIL ET RÉDUCTION DES COÛTS
- ASSURANCE D'UNE QUALITÉ TOTALE
- DU VOL D'AUTORISATIONS, DES DROITS, DES MANIPULATION DE PROTOCOLE, DES FONCTIONS D'ENREGISTREMENT, DE LA MÉMOIRE, ...
- DÉTECTION D'ACTIVITÉS SUSPECTES OU DE CAS D'EXTRUSIONS PAR L'INSTALLATION DE LOGICIELS PIÉGÉS
- AVERTISSEMENTS ET RÉACTIONS AUTOMATIQUES
- AUDIT ET VÉRIFICATION DE LA CONFORMITÉ
- SURVEILLANCE DES FICHIERS AVEC UN RAPPORT DES CHANGEMENTS
- SURVEILLANCE D'INTRUSIONS ET D'ACCÈS EXTERNES NON AUTORISÉS
- DÉTECTION DES INTRUS ET DES INITIÉS
- DÉTECTION D'INTRUSIONS ET D'ACCÈS EXTERNES NON AUTORISÉS
- FIDÈLE AUX STANDARDS LÉGAUX TELS QUE SOX, KONTRAG, ISO, BS, U.S. DOD, ...
- ASSISTANCE EFFICACE POUR TOUS LES DÉPARTEMENTS
- RAPPORTS INCLUANT UN SYSTÈME DE POINTS
- PERMET L'ASSOCIATION AVEC DES SYSTÈMES DE TICKET, DE GESTIONS DES PROBLÈMES ET D'AUTRES SYSTÈMES ITIL
- POSSIBILITÉ D'UN RAPPORT PERSONNALISÉ
- PROTECTION ET DÉFENSE CONTRE LES ABUS ET LES ATTAQUES
- INTERFACES OUVERTES PERMETTANT UNE INTÉGRATION FACILE
- ANALYSE CONSTANTE DES POINTS FAIBLES PAR UNE SIMULATION D'INTRUSION, ET DONC SANS CONSÉQUENCES DOMMAGEABLES
- VÉRIFICATION DE LA QUALITÉ DU MOT DE PASSE
- PERMET L'ENCAPSULATION DES APPLICATIONS COMME UNE MESURE EFFICACE CONTRE LES ATTAQUES COMME ENTRE AUTRES BUFFER OVERFLOW, FORMAT STRING, ...
- COMPATIBLE AVEC TOUTES SORTES DE SOURCES TELLES QUE SMF, LOGS, ETC.
- POUR LA SÉCURITÉ ET LA RÉVISION
- INSTRUCTIONS ÉTENDUE FOURNIES
- RÉSULTATS (LOGS, REPORTS, ETC.) SÉCURISÉS CONCERNANT L'AUDIT
- SIMULATION (PAR EXEMPLE IPL)
- VÉRIFICATION SYNTAXIQUE ET SÉMANTIQUE DU ENSEMBLE DES DONNÉES SYSTÈMES COMME P.E. PARMLIB, VTAMLST, ETC.
- UTILISATION ENTIÈREMENT AUTOMATISÉE
- INTÉGRATION AISÉE DANS LES SYSTÈMES DE SÉCURITÉ ET DE MANAGEMENT MULTI-PLATE-FORME (SYMANTEC, CA, TIVOLI ETC.) GRÂCE AUX KITS DE CONNEXION



PAR UNE SURVEILLANCE ET UNE SÉCURITÉ INTENSIVES, SF-SHERLOCK INSTALLE UN BOUCLIER PROTECTEUR AUTOUR DE LA PLATE-FORME z GRÂCE À SON SYSTÈME DE SURVEILLANCE ET DE SÉCURITÉ.

ENTREPRISE

- **Normes et instructions légales**
- **Avertissements et réactions automatiques**
- **Enregistrement sécurisé par audit**
- **Association et intégration**
- **Rapports**
- **...**

SOLUTION: SURVEILLANCE DE LA SÉCURITÉ ET DE LA QUALITÉ EN TEMPS RÉEL AVEC SF-SHERLOCK

»Technologie: SF-Sherlock représente la technologie la plus performante **dans le domaine de la surveillance en temps réel dans la mesure où il assure une sécurité complète et une qualité automatiques** sur la plate-forme z en intégrant la surveillance, l'enregistrement, l'avertissement, la réaction, le rapport et la possibilité d'une simulation (par exemple IPL) Le tout avec une solution globale et complète. Grâce à ces modules, SF-Sherlock est un processus automatique et permanent qui surveille et analyse le système de sécurité (le serveur de sécurité ou RACF, ainsi que CA-TSS et CA-ACF2), des processus spécifiques et des sous-systèmes (DB2, LDAP, etc.) ainsi que le système z/OS avec tous ses composants. Il détecte de façon sûre des changements pertinents et informe la personne compétente en temps et en heure, par e-mail ou SMS, de l'événement s'étant produit, tels que des erreurs, attaques, manipulations, etc. L'audit réalise en correspondance une surveillance automatisée en continue, fournissant un rapport et une évaluation. Ceci dispense le client des manipulations de résultats laborieuses en gagnant du temps avec des procédures entièrement automatisées. **Vous bénéficierez ainsi de plus de liberté, de flexibilité et de sécurité**. SF-Sherlock peut d'autre part dépasser le simple rapport et réagir immédiatement dans des cas précis; il peut par exemple rejeter instantanément des intrus hors du système. Ce contrôle permanent de votre système vous assure une **protection 24h/24**. Le niveau de sécurité et de qualité atteint vous garantit une maîtrise totale de votre système, tout en réduisant les coûts.

»La nécessité de réagir est indéniable: Depuis 2004, le bureau allemand pour la sécurité informatique (BSI) va bien au-delà du niveau de suivi du département U.S. de la défense en parlant ouvertement des risques et en définissant les mesures de sécurité nécessaires pour la plate-forme z/OS dans son guide intitulé «IT Baseline Protection Manual». La demande clé est la description de **l'exigence »d'une utilisation d'une surveillance de sécurité en temps réel pour le système z/OS afin de pouvoir détecter plus rapidement les délits en matière de sécurité«**. Une surveillance en temps réel uniquement pour un aspect isolé de la sécurité, tels que les enregistrements SMF, est encore insuffisante. Surveiller le système z/OS dans son ensemble, avec tous ses composants, ses relations complexes et ses détails est nécessaire. SF-Sherlock surveille le système z/OS de manière globale et complète. Le principal danger réside dans les procédures «sournoises» passées inaperçues et les failles dissimulées dans le z/OS, telles que l'obtention de plus hautes autorisations, la destruction d'audit ou d'un accès aux ressources non-contrôlé. Les professionnels peuvent ainsi espionner sans se faire remarquer toutes les données par un détournement et une manipulation du système de sécurité sans même laisser un simple enregistrement SMF ou log. De façon analogue, des erreurs de paramètres ou de configuration du système restés inaperçus remettent en question la disponibilité du système, jusqu'au prochain IPL. Les déficits concernant la sécurité et la qualité représentent des catastrophes qu'il faut éviter « à tout prix ». Par conséquent, **SF-Sherlock vérifie automatiquement votre système de sécurité ainsi que le parmlib ou d'autres systèmes de données importantes de système pour scrutant toute éventuelle faille ou erreur** après chaque modification survenue dans votre système. Une technologie en temps réel est nécessaire car la durée des activités professionnelles illégales est extrêmement courte – la détection, les mesures de prévention et la présentation des preuves ne peuvent être effectuées autrement. La liste des faiblesses et des erreurs possibles est si grande que seule une surveillance entièrement automatisée peut permettre d'atteindre les objectifs fixés.

»Une technologie qui garantit le succès: La technologie automatique et globale de SF-Sherlock concernant la sécurité et l'assurance de qualité est tout à fait en accord avec les objectifs de la sécurité informatique mentionnés ci-dessus. Elle permet à votre plate-forme mainframe d'être conforme aux différentes réglementations et procédures légales. Avec SF-Sherlock, vous ne vous contentez pas de répondre aux exigences nécessaires: vous alliez **une assurance de qualité totale à une protection globale**. SF-Sherlock représente le chemin sécurisé de l'avenir de votre entreprise. Une surveillance et un examen constants et complets, spécialement à des niveaux techniques élevés, vont devenir incontournables avec les nouvelles fonctions du z/OS (Unix System Services, Sysplex Technologie, etc.) et les nouveaux domaines d'application tels que le serveur web, le serveur de partage de données et la plate-forme de commerce électronique. Il est indéniable que les mesures standards de sécurité semblent de plus en plus insuffisantes. **La fonction SF-Sherlock comme système de détection des intrusions et des accès externes non sollicités assure une protection efficace contre les attaques internes et externes**. Il s'agit même du système représentant le plus haut niveau de protection contre l'ouverture grandissante vers l'extérieur de systèmes et de réseaux auparavant fermés. Avec sa technologie de pointe, SF-Sherlock est une étape essentielle dans le maintien d'une sécurité et d'une qualité constantes à un niveau élevé permettant de combattre ces risques.

»Productivité assurant le succès: En tant que processus automatique fonctionnant en temps réel, SF-Sherlock travaille dans les domaines de l'administration de la sécurité, de la surveillance du système, de la sécurité informatique, ainsi que dans la protection des données et des informations. En outre, il intègre ces éléments dans un processus workflow hautement efficace, vous offrant **une plus forte productivité et une réduction notable des coûts**. SF-Sherlock assure une sécurité globale pour toute l'entreprise, même dans un contexte multi-plate-forme. Sa valeur ajoutée vous fournie une rentabilité accrue et une efficacité en coût pour toutes les personnes impliquées. Le concept d'implémentation «plug and play» vous permet d'atteindre cet objectif et le travail correspondant, tout en vous libérant des préoccupations légales, et ce dans un minimum de temps, coût et effort.

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM