SF-SHERLOCK®

SU OBJETIVO

MÁXIMA SEGURIDAD
MÁXIMA CALIDAD
EN LA Z-PLATAFORMA
POR AUTOMATIZACIÓN CON
UN MÍNIMO DE ESFUERZO

PROTECCIÓN TÉCNICA Y
LEGAL POR UN CONTROL
DETALLADO Y COMPLETO
EN TIEMPO REAL

» UNA DE LAS INNOVACIONES MÁS FUNDAMENTALES EN EL SECTOR DE LA SEGURIDAD DEL MAINFRAME DESDE EL RACF. «

CONTROL TOTAL DE SEGURIDAD Y CALIDAD EN LA Z-PLATAFORMA

Usted es consciente de los riesgos y peligros actuales, y por eso valora al máximo la seguridad informática para proteger el capital de su empresa. En la era de Internet y comercio electrónico usted quiere seguir confiando en la idea »mainframe = seguridad máxima«.

Usted conoce las actuales y estrictas regulaciones y recomendaciones legales, como BASEL II, el Manual de »Protección fundamental en Tecnología Informática« (Ministerio Alemán de Seguridad de Tecnología Informática), 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. y los criterios de certificación según ISO o BS. Estas normas exigen a su empresa la aplicación de medidas precisas, eficaces y efectivas para asegurar todos los procesos basados en la tecnología informática y su auditoría correspondiente – incluyendo la tecnología subyacente – contra ataques internos y externos. **Además necesita pruebas claras para clientes, accionistas y la legislación** comprobando que se ha hecho todo lo posible – técnica y legalmente – para garantizar el nivel máximo de seguridad y calidad, y también para conseguir **una buena evaluación [de riesgos].** Su objetivo para el mainframe de su empresa es cumplir con todas estas exigencias legales y técnicas con el mínimo esfuerzo. Por eso usted busca una solución detallada y completa que trabaje automáticamente, técnicamente con la máxima eficiencia, legalmente aceptada y con una auditoría segura.

Usted considera la seguridad, la calidad y la eficiencia de costes como factores de competitividad altamente importantes. Usted sabe que solamente con la máxima calidad y el máximo nivel de automatización en los procesos de trabajo diarios puede conseguir la más alta productividad exigida, creando así la flexibilidad y el tiempo necesarios para afrontar los actuales cambios empresariales y las futuras oportunidades.

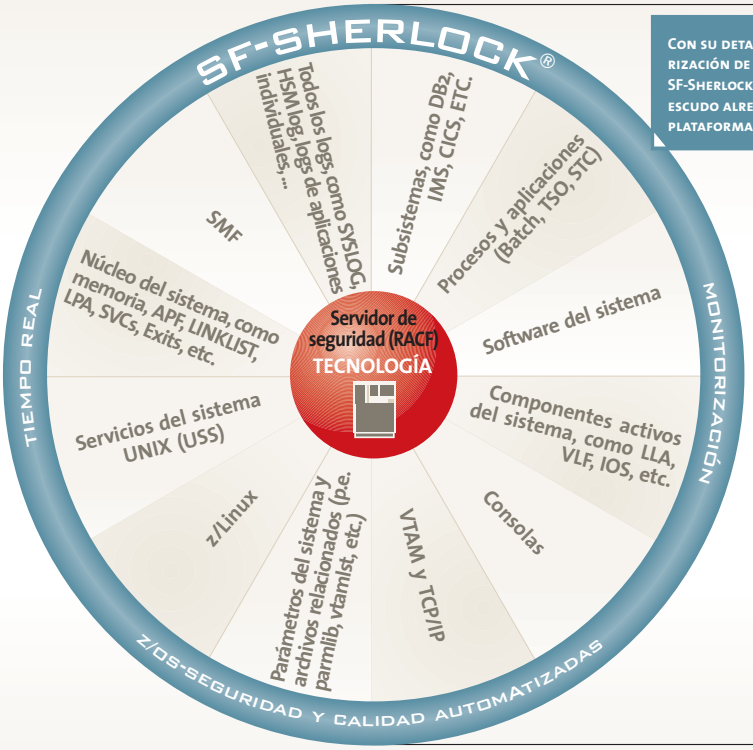
Usted quiere una solución única que realice todas las tareas necesarias, como control de incidentes, análisis de los puntos débiles de su sistema mediante una evaluación permanente de vulnerabilidades y prácticamente cubriendo **todo el entorno técnico de la plataforma mainframe.** Al mismo tiempo, dentro de su deseado nivel de valor añadido, esta solución debería permitir una aplicación diaria y una cooperación organizada entre todos los departamentos, **desde el nivel técnico hasta el nivel más alto de gestión.**

Además, usted exige la posibilidad de integración en la gestión de seguridad de la empresa entera y las soluciones de auditoría. Usted nunca quiere dudar de sus inversiones en estos entornos. La solución que usted exige debe apoyar sistemáticamente sus intereses, también dentro del marco de **ITIL, COBIT, BS7799,** entre otros.

Z-SEGURIDAD Y CALIDAD AUTOMATIZADAS CON SF-SHERLOCK ES LA RESPUESTA A LOS NUEVOS CAMPOS DE Z-APLICACIONES EN LA ERA DE INTERNET Y COMERCIO ELECTRÓNICO

RENDIMIENTO

- PROTECCIÓN DE 24 HORAS POR UN CONTROL EN TIEMPO REAL
- CONTROL DE APLICACIONES
- REDUCCIÓN DE TRABAJO Y GASTOS
- GARANTÍA TOTAL DE CALIDAD
- DETECCIÓN DE ABUSOS DE AUTORIZACIÓN Y MANIPULACIONES (DINÁMICAS) DE LAS FUNCIONES DEL PROTOCOLO Y DEL REGISTRO, DE LA MEMORIA, ...
- DETECCIÓN DE ACTIVIDADES SOSPECHOSAS Y DE EXTRUSIÓN POR LAS ASÍ LLAMADAS TRAMPAS LÓGICAS
- NOTIFICACIÓN Y REACCIÓN AUTOMÁTICAS
- REVISIÓN Y AUDITORÍA DE INTEGRIDAD
- MONITORIZACIÓN DE FICHEROS CON DELTA-INFORMES
- MONITORIZACIÓN DE INTRUSOS Y USUARIOS INTERNOS
- DETECCIÓN DE INTRUSIÓN Y EXTRUSIÓN
- CUMPLIMIENTO DE NORMAS LEGALES COMO SOX, KONTRAG, ISO, BS, U.S. DOD, MINISTERIO ALEMÁN DE SEGURIDAD INFORMÁTICA (BSI), ...
- MÁXIMO APOYO PARA TODOS LOS DEPARTAMENTOS
- INFORMES INCLUYENDO PUNTUACIONES
- POSIBILIDAD DE ACOPLARSE A SISTEMAS DE TICKET, CON PROBLEMAS U OTROS ITIL-SISTEMAS
- INFORMES ESPECÍFICOS PARA CADA CLIENTE
- PROTECCIÓN Y DEFENSA CONTRA USO INDEBIDO
- INTERFACES ABIERTAS PARA UNA INTEGRACIÓN FÁCIL
- ANÁLISIS PERMANENTE DE PUNTOS DÉBILES CON UNA PENETRACIÓN SUAVE SIN POSIBLES INTERFERENCIAS
- PRUEBAS DE CALIDAD DE CONTRASEÑAS
- CAPAS DE APLICACIONES COMO MEDIDA CONTRA ATAQUES COMO BUFFER OVERFLOW, FORMAT STRING, ETC.
- APOYO PARA TODO TIPO DE FUENTE, COMO SMF, LOGS, ...
- AMPLIAS POLÍTICAS DE SEGURIDAD
- RESULTADOS SEGUROS DE AUDITORÍA (LOGS, INFORMES, ETC.)
- SIMULACIÓN (P.E. IPL)
- ANÁLISIS SINTÁCTICO Y SEMÁNTICO DE ARCHIVOS DEL SISTEMA, COMO PARMLIB, VTAMLST, ETC.
- FUNCIONAMIENTO TOTALMENTE AUTOMATIZADO
- KITS DE CONEXIÓN PARA UNA INTEGRACIÓN FÁCIL EN LA SEGURIDAD DE MÚLTIPLES PLATAFORMAS ENTRELAZADAS Y LAS SOLUCIONES DE LA GESTIÓN DEL SISTEMA, COMO SYMANTEC, CA, TIVOLI, ETC.



EMPRESA

- **Políticas y normas legales**
- **Notificación y reacción automáticas**
- **Registro de una auditoría segura**
- **Acoplamiento e integración**
- **Informes**
- **...**

LA SOLUCIÓN: SF-SHERLOCK MONITORIZACIÓN EN TIEMPO REAL

»Tecnología: SF-Sherlock representa la tecnología de alto rendimiento de **monitorización en tiempo real para establecer una automatización completa de seguridad y calidad** en la z-plataforma integrando el control, la grabación, la notificación, la reacción, los informes y las posibilidades de simulación (p.e. IPL) en una solución única. Con sus componentes, SF-Sherlock es un proceso permanente dentro del sistema que controla y examina el sistema de seguridad (el servidor de seguridad o RACF tanto como CA-TopSecret y CA-ACF2), procesos específicos y subsistemas (DB2, LDAP, etc.) tanto como el sistema operativo del z/OS y todos sus componentes. Graba cambios relevantes de manera segura e informa a la persona responsable a tiempo y específicamente de los incidentes relacionados con su sector, como errores, ataques, manipulaciones, cambios, etc., por ejemplo mediante e-mail o SMS. Correspondientemente, el departamento de auditoría consigue continuamente un control y una evaluación automatizados, incluyendo informes. Esto significa que nadie tiene que procesar manualmente los resultados y perder tiempo con tareas rutinarias, porque todos los procesos están completamente automatizados. **Esto le da libertad, flexibilidad y seguridad**. SF-Sherlock va más allá de simples informes en casos determinados. Por ejemplo, con su optativa reacción automática e instantánea, SF-Sherlock tira intrusos inmediatamente del sistema. Con este control y observación permanentes en el sentido de una **protección de 24 horas**, usted consigue el máximo nivel necesario de seguridad y calidad que le permite dominar su sistema y reducir costes.

»La necesidad de actuar es indiscutible: Desde 2004, el Ministerio Alemán de Seguridad Informática (BSI) – con su Manual de Seguridad »Protección fundamental en Tecnología Informática« – va mucho más allá de las normas del Ministerio Estadounidense de Defensa, analizando abiertamente los riesgos y definiendo las medidas de seguridad necesarias para la plataforma del z/OS mainframe. El mensaje principal describe **la demanda de »utilizar una monitorización de seguridad en tiempo real de sistemas de z/OS para poder determinar más rápido violaciones de seguridad«**. Una monitorización en tiempo real de un único aspecto aislado de seguridad, como los protocolos SMF, es aún insuficiente. Es necesaria una monitorización del z/OS entero con todos sus componentes y relaciones y detalles complejos. SF-Sherlock controla el sistema de z/OS detallada y completamente, ya que el peligro más grande viene por procesos difíciles que pasan desapercibidos y errores ocultos en algún lugar dentro del z/OS, como conseguir una autorización más alta, romper el proceso de auditoría u obtener acceso desapercibido a recursos. De esta manera, expertos pueden espiar todos los datos evitando y manipulando el sistema de seguridad sin dejar rastro de un único protocolo en el SMF o el registro. Correspondientemente, parámetros y configuraciones erróneos del sistema que pasan desapercibidos pueden poner en peligro la disponibilidad de todo el sistema, por lo menos hasta la próxima IPL. Tanto las faltas de seguridad como las de calidad representan una catástrofe y tienen que ser evitadas »a todo coste«. Por eso, después de cada modificación dentro del sistema, **SF-Sherlock analiza automáticamente su sistema de seguridad tanto como el parmlib y otros archivos importantes en busca de posibles cambios o errores**. Una tecnología en tiempo real es necesaria porque la vida de manipulaciones para actividades ilegales profesionales es extremadamente corta – detección, impedimento mediante reacción y constante presentación de pruebas no son posibles de otra manera. La lista de posibles vulnerabilidades y errores es larguísima y solamente se puede conseguir con un control totalmente automatizado.

»Tecnología que garantiza éxito: La tecnología automática y completa para la garantía de seguridad y calidad de SF-Sherlock apoya completamente los objetivos arriba mencionados y hace que su plataforma de mainframe cumpla con todas las normas legales. Con SF-Sherlock, usted no sólo encuentra los requisitos necesarios sino también consigue una **garantía total de calidad y una protección completa**. SF-Sherlock prepara el camino de seguridad para el futuro de su empresa. El control y el análisis constantes y completos, especialmente a niveles técnicos más profundos, cada vez es más importante con las funciones nuevas del z/OS (Unix/USS, Sysplex, etc.) y las áreas nuevas de aplicaciones como servidores de red, servidores de datos y plataformas de comercio electrónico. No cabe duda de que las medidas estándares así cada vez parecen más insuficientes. La función de **SF-Sherlock como sistema de detección de intrusión y extrusión para la defensa contra ataques internos y externos** es aún más importante al nivel más alto de protección contra la apertura creciente de sistemas y redes hasta ahora cerrados. Con su tecnología líder, SF-Sherlock es un paso esencial para conseguir un nivel de seguridad y calidad constante y actual para combatir estos riesgos.

»Productividad que garantiza éxito: Como proceso automático en tiempo real, SF-Sherlock trabaja tanto para los departamentos de seguridad y auditoría y la protección de datos e información como para el departamento de tecnología del sistema. Es más, los integra en un proceso común y altamente eficiente que lleva a **una productividad más alta y una reducción importante de gastos**. Por su automatización completa de seguridad y calidad, SF-Sherlock es una solución íntegra para toda la empresa, también en entornos de plataformas múltiples. Su valor añadido proporciona la rentabilidad más alta y eficacia de costes para todos los involucrados. Con el concepto de Plug&Play-Implementation, usted consigue este objetivo reduciendo trabajo y cumpliendo con las normas legales con un mínimo de tiempo, costes y esfuerzo.

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM