SF-SHERLOCK®

IHR ZIEL

HÖCHSTE SICHERHEIT
HÖCHSTE QUALITÄT
AUF DER Z-PLATTFORM
DURCH AUTOMATION MIT
MINIMALEM AUFWAND

TECHNISCHE UND
RECHTLICHE ABSICHERUNG
DURCH REALTIME-
ÜBERWACHUNG

» EINE DER WESENTLICHSTEN INNOVATIONEN DER MAINFRAME-SICHERHEIT SEIT EINFÜHRUNG VON RACF. «

GANZHEITLICHE ÜBERWACHUNG DER Z-PLATTFORM

Sie sind sich der heutigen Gefahren und Risiken bewusst und gestehen höchster Sicherheit in der Datenverarbeitung und dem in ihr liegenden Unternehmenskapital einen sehr hohen Stellenwert zu. Auf die These »Mainframe = Sicherheit« möchten Sie weiterhin vertrauen können, und dies auch im Zeichen von Internet und E-Commerce.

Sie kennen die aktuellen strengen gesetzlichen Regelungen und Empfehlungen, wie Basel II, KonTraG, BSI-Grundschutz, Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), RS FAIT 1, HIPAA Security, 95/46/EC Data Protection Directive, etc. und die **Zertifizierungskriterien nach ISO oder BS**. Diese fordern von Ihrem Unternehmen – **auch für ein gutes Rating** – präzise und effizient wirksame Massnahmen zur Absicherung sämtlicher IT-basierter Prozesse gegen Angriffe von innen und aussen, z. B. das BSI: »Praktisch unverzichtbar sind solche Detektionsmassnahmen, wenn im Schadensfall sehr grosse Schäden bis hin zum Personenschaden zu erwarten sind.« (BSI-Grundschutzhandbuch 2004, Abschnitt M6.67). Automatisch arbeitende, juristisch ausreichende, technisch wirksame und revisionssichere Überwachungs- und Kontrollprozesse sind Ihr Ziel.

Sie stufen Sicherheit, Qualität und Kosteneffizienz als äusserst wichtige Wettbewerbsfaktoren ein und wissen, dass nur mit einer gesteigerten Qualität und hochgradigen Automation in den täglichen Arbeitsprozessen die geforderte höhere Produktivität und damit der notwendige Freiraum für die eigentlich neuen Herausforderungen der Zukunft geschaffen werden können.

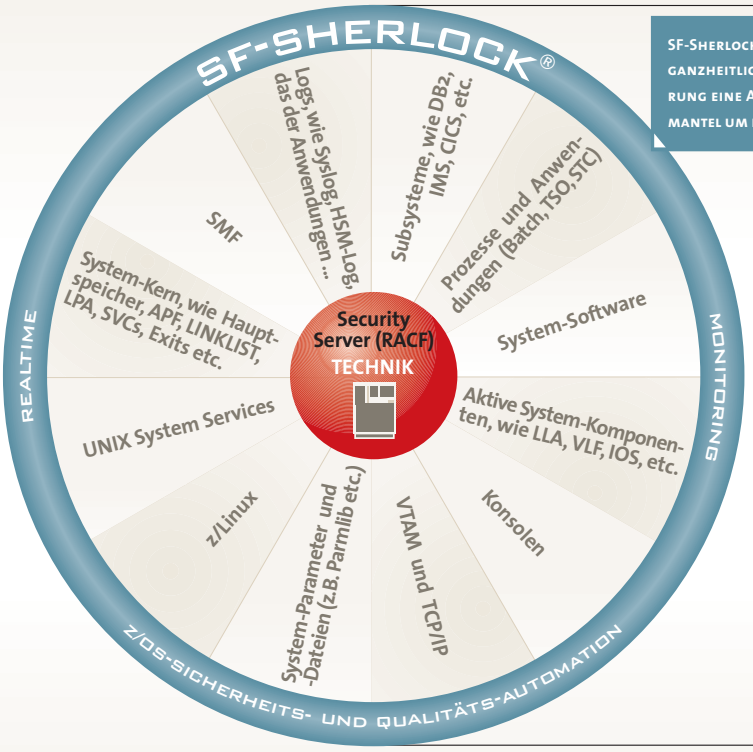
Sie wünschen sich eine Lösung, die bezüglich der Event-Überwachung und Schwachstellenprüfung **ganzheitlich die gesamte technologische Breite der Mainframe-Plattform** vollständig abdeckt, und gleichzeitig in ihrer Wertschöpfungshöhe eine tägliche Anwendung und organisatorische Zusammenarbeit **von der technischen Ebene bis hin zum oberen Management** abteilungsübergreifend erlaubt.

Sie verlangen auch die Offenheit zur Integration in unternehmensweite Security-Management- und Audit-Lösungen und möchten Ihre Investitionen in diesem Umfeld nicht in Frage stellen, sondern ihre Interessen konsequent unterstützt wissen, z.B. auch im Rahmen von **ITIL, COBIT, BS7799** o.ä.

Z-SICHERHEITS- UND QUALITÄTS-AUTOMATION MIT SF-SHERLOCK ALS ANTWORT AUF DIE NEUEN Z-EINSATZFELDER INTERNET UND E-BUSINESS

LEISTUNG

- 24-STUNDEN-SCHUTZ DURCH REALTIME-MONITORING
- ANWENDUNGSÜBERWACHUNG
- ARBEITSENTLASTUNG UND KOSTENREDUKTION
- AUFDECKUNG VON BERECHTIGUNGS-MISSBRAUCH UND (DYNAMISCHEN) MANIPULATIONEN AN DEN PROTOKOLLIERUNGS- UND LOG-FUNKTIONEN, AM SPEICHER, ...
- AUFFÄLLIGKEITS- UND EXTRUSION-DETEKTION DURCH SOGENANNTE LOGISCHE FALLEN
- AUTOMATISCHE BENACHRICHTIGUNG UND REAKTION
- COMPLIANCE-PRÜFUNG UND AUDITING
- EVENT- UND STATUS-AUDITING
- INTRUDER- UND INSIDER-MONITORING
- INTRUSION- UND EXTRUSION-DETECTION
- ZUR ERFÜLLUNG VON SOX, KONTRAG, ISO, BS, BSI-GRUNDSCHUTZ, ...
- AUCH FÜR IT-REVISION UND AUDITING
- REPORTING UND KENNZAHLENSYSTEME
- KOPPLUNG AN TICKET-, PROBLEM- UND ANDERE ITIL-SYSTEME MÖGLICH
- MANDANTENFÄHIGES REPORTING
- MISSBRAUCHSSCHUTZ UND -ABWEHR
- OFFENE SCHNITTSTELLEN ZWECKS INTEGRATION
- KAPSELN VON ANWENDUNGEN ALS MASSNAHME GEGEN ATTACKEN, WIE BUFFER OVERFLOW, FORMAT STRING O.Ä.
- PASSWORD-QUALITÄTSPRÜFUNG
- PERMANENTE SCHWACHSTELLENANALYSE (VULNERABILITY ASSESSMENT) IM SINNE EINER STÖRUNGSFREIEN SOFT-PENETRATION
- UNTERSTÜTZUNG SÄMTLICHER QUELLEN, WIE SMF, LOGS, ...
- MITGELIEFERTE UMFASSENDE POLICIES
- REVISIONSSICHERHEIT
- SIMULATION (Z.B. IPL)
- SYNTAX- UND SEMANTIK-PRÜFUNG FÜR SYSTEMDATEIEN (Z.B. PARMLIB, VTAMLST, ETC.)
- VOLLAUTOMATISCHER BETRIEB, KEIN MANUELLES ARBEITEN
- z = z/OS + z/Linux
- z/OS = MVS + UNIX



SF-SHERLOCK LEGT MIT DER GANZHEITLICHEN ABSICHERUNG EINE ART SCHUTZMANTEL UM DIE Z-PLATTFORM

BUSINESS

- **Policies und gesetzliche Auflagen**
- **automatische Benachrichtigung u. Reaktion**
- **Revisionssichere Aufzeichnung (Logs)**
- **Kopplung**
- **Reporting**
- ...

LÖSUNG: SF-SHERLOCK REALTIME-SECURITY-MONITORING

»Technologie:___SF-Sherlock repräsentiert die leistungsstarke **Realtime-Monitoring-Technologie zur ganzheitlichen Sicherheits- und Qualitäts-Automation** auf der z-Plattform, indem sie Überwachung, Aufzeichnung, Benachrichtigung, Reaktion, Reporting und die Möglichkeit zur Simulation (z.B. IPL) in eine Lösung integriert. Es ist ein im System automatisch laufender Prozess, der das Security-System (Security Server bzw. RACF, ebenso CA-TopSecret und CA-ACF2), spezifische Prozesse bzw. Subsysteme (DB2, LDAP, etc.) und das z/OS-Betriebssystem mit seinen Komponenten permanent überwacht, überprüft, relevante Veränderungen revisionssicher aufzeichnet, und betroffene Mitarbeiter individuell über definierte Ereignisse seines Bereichs, wie Fehler, Angriffe, Manipulationen, etc. just-in-time informiert, beispielsweise per E-Mail, SMS, etc. Die Abteilung Auditing erhält entsprechend eine zeitnahe automatisierte Überwachung und Bewertung, einschließlich Reporting. D.h. kein Mitarbeiter muss Ergebnisse manuell erarbeiten und sich in Routinearbeiten erschöpfen, alle Vorgänge sind vollständig automatisiert. Das schafft Freiraum und Sicherheit. Über das reine Reporting hinaus kann SF-Sherlock in definierten Fällen auch sofort selbständig reagieren, z.B. um unbefugte Eindringlinge im Sinne eines **24-Stunden-Schutzes** sofort aus dem System zu werfen. Mit dieser permanenten Kontrolle und Beobachtung (K&B) erlangen Sie die notwendige Souveränität über Ihr System und die geforderte Sicherheit.

»Der Handlungsbedarf ist unbestritten:___Seit 2004 definiert das Deutsche **Bundesamt für Sicherheit in der Informationstechnik (BSI)** auch die für die Mainframe-Plattform notwendigen Absicherungsmaßnahmen in seinem zentralen Werk, dem **IT-Grundschutzhandbuch**. Zentrale Aussage ist die **Aufforderung zum »Einsatz eines Security-Realtime-Monitors für z/OS-Systeme, um Sicherheitsverletzungen schneller feststellen zu können«**. Die dominante Gefahr besteht in den unbemerkten Vorgängen und verdeckten Fehlern, insbesondere in den dynamischen (Speicher-) Manipulationen, z.B. zur Erlangung höherer Berechtigungen und dem unbemerkten Ressourcen-Zugriff. Dies gilt für Security und Systemtechnik gleichermaßen. So können Profis durch gezieltes Umgehen und Manipulieren des Security-Systems alle Daten unbemerkt ausspionieren; entsprechend stellen unbemerkt bleibende, fehlerhafte Systemparameter und –konfigurationen die Verfügbarkeit der Systeme in Frage. Beides stellt gleichermaßen Katastrophen dar, und derartige Gefahren gilt es um jeden Preis zu verhindern. Eine Realtime-Technologie ist notwendig, weil die Lebensdauer von Manipulationen für professionelle illegale Aktivitäten extrem kurz ist – Erkennung, Verhinderung durch Reaktion und Beweisführung sind auf anderem Weg nicht möglich. Die Checkliste des notwendigen Misstrauens und Überprüfens ist so umfassend, dass nur eine ganzheitliche automatisierte Überwachung zum Ziel führt.

»Erfolgsgarant Technologie:___Die automatisch arbeitende und umfassende Sicherheits- und Qualitätssicherungs-Technologie von SF-Sherlock unterstützt vollständig die Zielsetzung und Umsetzung des IT-Grundschutzes, und geht im Sinne Ihres Unternehmens zukunftsweisend weit darüber hinaus. Die **permanente ganzheitliche Überwachung und Überprüfung**, insbesondere auch auf tiefer technischer Ebene, wird mit den neuen Funktionen des z/OS (Unix-System-Services, Sysplex-Technologie etc.) und den sich hieraus ergebenden Einsatzgebieten als Webserver, Datenserver und E-Commerce-Basis zusätzlich zu den bisherigen Standard-Maßnahmen immer wichtiger. Auch die zunehmende Öffnung bisher geschlossener Systeme und Netze nach außen macht die SF-Sherlock-Funktion als Eindringungs- und Ausdringungserkennungssystem (Intrusion und Extrusion Detection) zur Abwehr interner und externer Angriffe als höchste Stufe der Absicherung immer bedeutender. SF-Sherlock ist mit seiner führenden Technologie ein wichtiger Schritt zur zeitgemäßen Sicherheit und Qualität und ist damit auch ein klarer Entlastungsnachweis gegenüber Kunden, Aktionären und dem Gesetzgeber, das heute technisch mögliche und rechtlich notwendige hierfür getan zu haben, auch im Rahmen der neuen Gesetzgebungen und Zertifizierungsanforderungen.

»Erfolgsgarant Produktivität:___Als automatisch arbeitender Realtime-Prozess arbeitet SF-Sherlock den Abteilungen Security-Administration und -Auditing, System-Technik und IT-Security als auch der IT-Revision und dem Datenschutz zu – dies führt zu hoher Produktivität und deutlicher Kostenreduktion. SF-Sherlock ist durch seine ganzheitliche Sicherheits- und Qualitäts-Automation eine integrierte Gesamtlösung für das ganze Unternehmen und durch seine hohe Wertschöpfung bei allen Beteiligten von hoher Wirtschaftlichkeit. Mit dem **Plug&Play-Implementierungskonzept** erreichen Sie dieses Ziel und die entsprechende arbeitsmäßige wie auch rechtliche Entlastung mit minimalem Zeit- und Kostenaufwand.

»Offenheit:___Der Kopplung von SF-Sherlock an andere Security- oder System-Management-Plattformen, wie z.B. von Symantec, CA, Tivoli etc. steht durch entsprechende **Connection-Kits** nichts im Wege.

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM