SF-SHERLOCK®

YOUR GOALS

HIGHEST SECURITY

HIGHEST QUALITY ON

THE ENTIRE Z PLATFORM

THROUGH AUTOMATION

WITH MINIMAL EFFORT

TECHNICAL PROTECTION

AND LEGAL COMPLIANCE

VIA COMPREHENSIVE

REAL-TIME MONITORING

» ONE OF THE MOST ESSENTIAL INNOVATIONS IN THE AREA OF MAINFRAME SECURITY SINCE RACF. «

COMPLETE SECURITY AND QUALITY MONITORING OF THE Z PLATFORM

You are aware of today's risks and dangers and therefore place a very high value on maximum IT security to protect your company's major assets. In the era of Internet and E-Commerce you want to keep trusting in the idea of »Mainframe = Highest Security«. ✓

You know the current, strict legal regulations and recommendations, such as Basel II, IT Baseline Protection Manual (German Federal Office for Information Security), 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. and the certification criteria according to ISO or BS. These standards require your company to apply precise, efficient and effective measures for securing all IT-based processes and related audit trails, including the underlying technology, against internal and external attacks. **You also need to have clear evidence of relief to customers, shareholders and legislators** by proving that everything possible, both technically and legally, has been done to ensure the highest standards in security and quality - also for the purpose of achieving a **good [risk] rating**. Your goal for your company's mainframes is to meet all these legal and technical requirements with minimal effort. This lets you search for a comprehensive solution that is automatically working, technically and highly effective, legally accepted, and audit-secure. ✓

You regard security, quality and cost efficiency as extremely important competitive factors. You know that only with increased quality and the highest level of automation in the daily work processes can you achieve the required highest productivity. Accomplishing this gives you the necessary flexibility and time to meet the »actual« business challenges and opportunities that the future brings. ✓

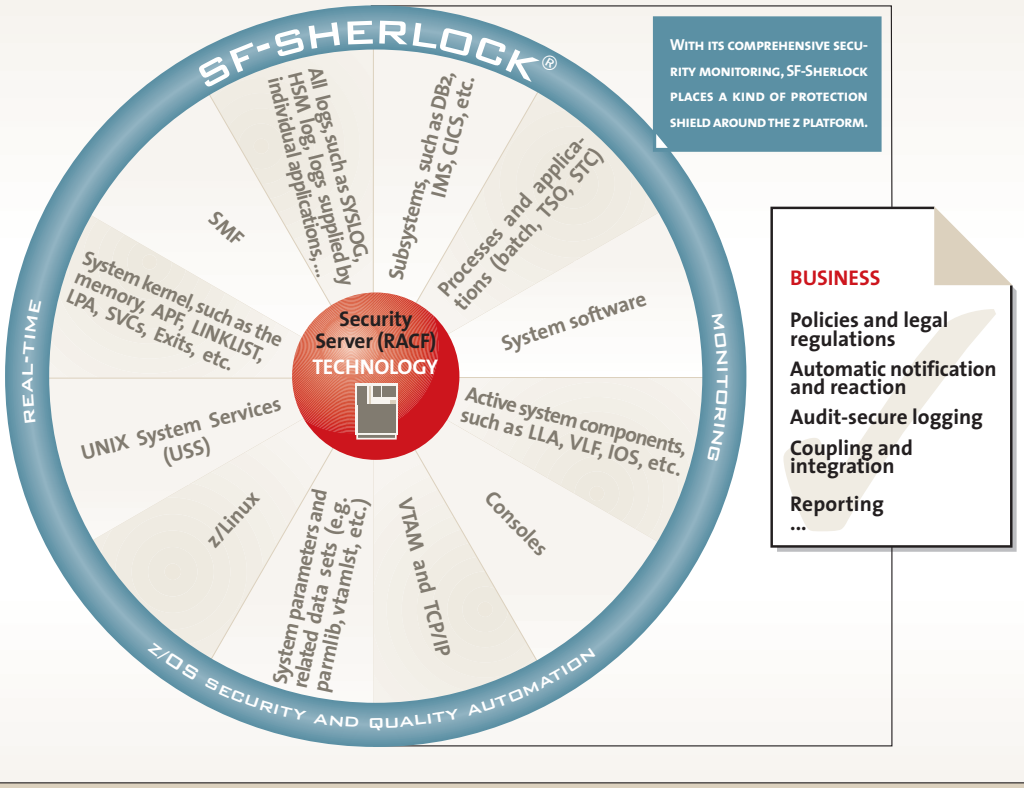
You want a single solution that performs all the necessary tasks, such as monitoring events, examining the weak areas of your system by a constant vulnerability assessment, and practically covering **the complete technological spectrum of the mainframe platform**. At the same time, in your desired level of increased value, this solution should allow a daily application and organized cooperation from all the different departments, namely **from the technical level up to the highest management level**. ✓

You also demand openness to integration into company-wide, cross-platform security management and audit solutions. You never want to doubt your investments in these areas. The solution you aim for should indeed consistently support your interests, also within the scope of **ITIL, COBIT, BS7799**, among others. ✓

Z SECURITY AND QUALITY AUTOMATION WITH SF-SHERLOCK IS THE ANSWER TO THE NEW Z APPLICATION FIELDS IN THE ERA OF INTERNET AND E-BUSINESS

PERFORMANCE

- 24-hour protection via real-time monitoring
- Monitoring of applications
- Work relief and cost reduction
- Total quality assurance
- Detection of authorization and privilege theft as well as any (dynamic) manipulation of the protocol and log functions, of the memory, ...
- Detection of suspicious activities or events as well as extrusion via so-called logical traps
- Automatic notification and reaction
- Compliance checking and auditing
- File monitoring with delta reporting
- Intruder and insider monitoring
- Intrusion and extrusion detection
- Compliance with legal standards, such as SOX, KonTraG, ISO, BS, U.S. DoD, German Federal Office for Information Security (BSI), ...
- Highly supportive for all departments
- Reporting including scoring
- Allows coupling to any ticket, problem and other ITIL-related systems
- Capable of client-specific reporting
- Protection and defence against misuse and tampering
- Open interfaces allow easy integration
- Constant trouble-free soft penetration in the sense of a constant vulnerability assessment
- Password quality testing
- Allows capsulation of applications as a powerful measure against attacks, such as buffer overflow, format string, among others
- Supports all types of sources, such as SMF, logs, ...
- Extensive policies provided
- Audit-secure results (logs, reports, etc.)
- Simulation (e.g. IPL)
- Syntax and semantic checks for system data sets, such as parmlib, vtamlst, etc.
- Fully automated operation
- Connection kits allow an easy integration in cross-platform security and system management solutions, such as of Symantec, CA, Tivoli, etc.



SOLUTION: SF-SHERLOCK REAL-TIME SECURITY AND QUALITY MONITORING

»Technology: SF-Sherlock represents the high performance **real-time monitoring technology for establishing complete security and quality automation** on the z platform by integrating the monitoring, recording, notification, reaction, reporting and the possibilities for simulation (e.g. IPL) into an overall solution. With its components, SF-Sherlock is a constantly running system process that monitors and examines the security system (Security Server or RACF as well as CA-TopSecret and CA-ACF2), specific processes and subsystems (DB2, LDAP, etc.) as well as the z/OS operating system with all its components. It records relevant changes in an audit-secure manner and informs the person concerned just in time and specifically about area-related events, such as errors, attacks, manipulations, changes, etc., for instance by e-mail or SMS. The auditing department correspondingly achieves continuously automated monitoring and rating, including reporting. This means no one has to manually process the results and waste time with routine tasks, since all procedures are fully automated. **This gives you freedom, flexibility, and security**. SF-Sherlock goes beyond pure reporting in well defined cases. For instance, with its optional automatic and instant reaction, SF-Sherlock throws intruders out of the system immediately. With this constant control and observation in the sense of **24-hour protection**, you achieve the required top-level of security and quality that lets you take command of your system and reduce costs.

»The demand for action can not be denied: Since 2004 the German Federal Office for Information Security (BSI) goes far beyond the compliance level of the U.S. Department of Defense by openly discussing the risks and defining the necessary security measures for the z/OS mainframe platform in its central security guide, the »IT Baseline Protection Manual«. The key message describes the **demand for »using a real-time security monitor for z/OS systems to be able to determine security infringements faster«**. Real-time monitoring for only a single isolated security aspect, such as SMF records, is still insufficient. Monitoring the entire z/OS with all its components and complex relations and details is necessary. SF-Sherlock monitors the z/OS system comprehensively and completely since the dominant danger comes from unnoticed »tricky« procedures and concealed errors anywhere in the z/OS, such as for reaching higher authorizations, breaking the audit trail, and obtaining unnoticed access to resources. In this way, professionals can spy on all data by targeted bypassing and manipulating the security system while not even leaving a single SMF or log record. Correspondingly, any unnoticed remaining erroneous system parameter or configuration may question the availability of the entire system, at the latest with the next IPL. Both security and quality deficits equally present catastrophes and must be prevented »at any cost«. Therefore, after each modification performed in the system, **SF-Sherlock automatically checks your security system as well as the parmlib and other important system files for any possible gap and error**. A real-time technology is necessary because the lifetime of manipulation for professional illegal activities is extremely short – detection, prevention through reaction, and the consistent presentation of evidence are not possible any other way. The checklist of possible vulnerability and errors is extensive and can only be fulfilled by completely automated monitoring.

»Technology that guarantees success: The automatic and comprehensive security and quality assurance technology of SF-Sherlock fully supports the above mentioned outstanding objectives and lets your mainframe platform comply with all the different legal regulations and requirements. With SF-Sherlock, not only do you meet the necessary requirements, but you also accomplish both **total quality assurance and comprehensive protection**. SF-Sherlock paves the secure way of the future of your business. Constant and complete monitoring and examining, especially at deeper technical levels, are becoming increasingly important with the new z/OS functions (Unix System Services, Sysplex Technology, etc.) and the new application areas, such as web server, data server and E-commerce platform. There is no doubt that standard measures thus gradually seem to be insufficient. **SF-Sherlock's function as an intrusion and extrusion detection system for the defence against internal and external attacks** is even more significant as the highest level of protection against the increasing opening of previously closed systems and networks to the outside. With its leading technology, SF-Sherlock is an essential step in attaining a constant, up-to-date level of security and quality for combating these risks.

»Productivity that guarantees success: As an automatic real-time process, SF-Sherlock works for the departments of security management and auditing, data and information protection as well as system technology. Furthermore, it integrates them into a common and highly efficient workflow, which leads to **higher productivity and significant cost reduction**. Through its comprehensive security and quality automation, SF-Sherlock is an integrated solution for the whole company, also in a cross-platform context. Its added value provides the highest profitability and cost effectiveness for everyone involved. With the plug&play implementation concept, you reach this goal and the corresponding work as well as legal relief with minimal time, cost and effort.

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM