SF-NOEVASION®

REAL-TIME
AUDIT & COMPLIANCE
PROVIDER FOR Z/OS

YOUR GOALS

ULTIMATE HARDENING,
STREAMLINING AND
CONSOLIDATION OF YOUR
AUDIT & SECURITY TRAILS

LOG - BLOCK - MODIFY

ALLOWS REPLACEMENT
OF PASSWORD AND
SECURITY EXITS

TARGET YOUR TRUE AUDITING & SECURITY ENEMIES!

Systems and processes never tell you the whole story. But complete and authentic logs are a prerequisite for both proper IT operation and complete auditing & compliance – including effective detection of fraud and abuse. You may not believe this, but essential and highly critical activity on your recognized z/OS mainframe simply does not come to your attention since it is not logged or properly protected.

The triad of smart and smooth z/OS command and system service verification includes logging, blocking and modifying. SF-NoEvasion for z/OS provides the ultimate hardening and transparency of your audit trails and security mechanisms against information suppression, bypassing, or fraud and abuse. It also improves and enhances critical security controls to allow highly precise and flexible decisions on their usage! Become the boss by finally knowing the complete story on what's happening on your z platform!

The plug & play **Real-Time Sniffer, Spool Monitor, File Watcher, Universal Log Scanner** and **Event Forwarder** finally lets you feed all your security and compliance monitoring applications with event data – with utmost completeness and speed. The included PC-based system for **Security Information and Event Management (SIEM)** provides a high-performance audit workflow. As an option, it lets you also include events of non-mainframe platforms, such as Windows, UNIX, Linux, etc.

Highest security and compliance levels for the z/OS mainframe platform are requested. All security and compliance standards, like SOX, PCI, ISO, FERC, DOD, HIPAA, etc., claim full (100%) transparency and the ability to audit completely all processes in your company's IT. Missing audit information represents a top-level risk, implying the impossibility of effectively detecting fraud, abuse and non-compliant behavior.

But how can incomplete logs be possible on platforms having received the highest levels of [security] certifications? Your fear is reasonable! Various processes may be involved, such as invalid system configurations, critical system services supporting "no logging" features, tricky log suppression, bypassed security mechanisms, and much more. High-value compliance certifications may easily become invalidated in cases of incomplete audit data. Skilled software vendors, staff, or parties with any malicious intent may easily dupe you by hiding the "actual truth", and, furthermore, putting into question your company's compliance and the legal protections of your auditing.

SF-NoEvasion includes the experience of penetrating and assessing mainframes for over a decade to achieve extremely secure environments. It provides comprehensive and smart command and system service verification to completely audit and protect all critical z/OS components, including Security Server (RACF), user authentication, user password change, console commands, FTP, and much more. At last, you don't have to put up with any potential weaknesses related to your audit trails, and you can finally achieve the highest level of automated controls and completeness in your compliance strategy!

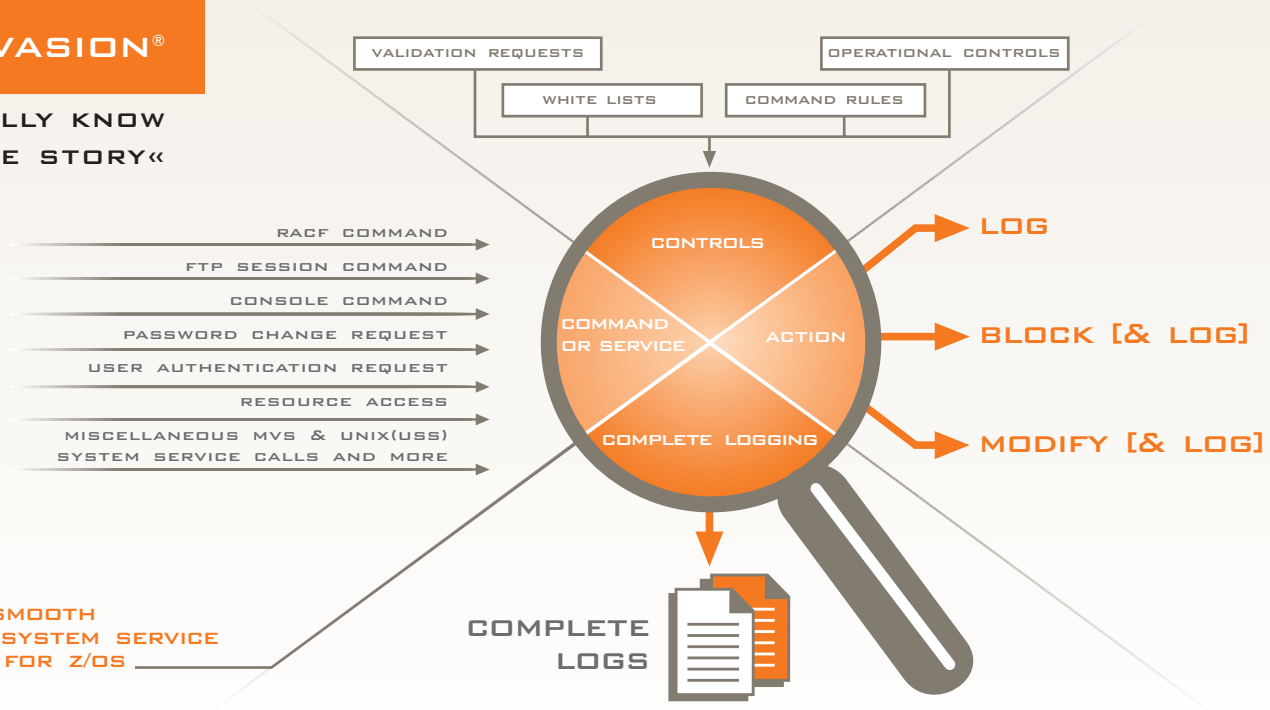
You finally know the whole story that is essential to becoming really compliant and secure!

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.com

REAL Z/OS SECURITY AND COMPLETE COMPLIANCE HAVE NEVER BEEN EASIER!

SF-NOEVASION®

»YOU FINALLY KNOW THE WHOLE STORY«



SMART AND SMOOTH COMMAND & SYSTEM SERVICE VERIFICATION FOR Z/OS

» Environmental and operational facts:

- SF-NoEvasion lets you review Security Server (RACF), console and FTP session commands as well as user authentication, user password changes, system command service calls, and much more.
- It is available for z/OS, and works in accord with all common security systems (Security Server (RACF), CA-ACF2 and CA-TSS). Some feature's availability depends on the security system in use.
- No operational risks are involved. SF-NoEvasion supports warning modes on several levels, and performs comprehensive reviews on its configuration before starting up, thereby avoiding any problems or damage.
- Highly flexible and precise white lists let you define all exceptions required by complex operational environments.
- Highly efficient programming techniques result in almost non-measurable CPU time consumption and no impacts.
- Strong self-monitoring guarantees constant consistency checking, attack detection, and highest availability.
- No kind of "Extra RACF", "Over RACF" becomes established questioning the transparency and effectiveness of your actual security controls. All SF-NoEvasion controls are completely transparent and easy to audit.

» Know the "whole truth" about what's really going on via fully-complete logging:

- SF-NoEvasion simply logs every critical event – this is important! No tricky suppression request will be honored anymore! Isn't it suspicious if system commands or resource accesses, for example, are performed without being logged?
- It constantly enables all audit and security relevant SMF records regardless of your system programmer's parmlib definitions. There is simply no reason to omit any critical SMF record at any time!
- Records service calls even when the operating system does not provide audit capabilities or allows callers to suppress logging. For example, LDAP's authentication via RACF will neither always create RACF SMF records nor update a user profile by the "last use date".
- Relieves you from the highly challenging "log all or nothing" decisions resulting from missing support of smooth selection capabilities and granular controls. For example, FTP either allows all users or none for any batch job (JCL) submission and spool access. Have you also been surprised that FTP does not record logon attempts with an invalid user ID, but only those with invalid passwords?

» Prevent all unauthorized activity via smart & smooth blocking:

- SF-NoEvasion's smart blocking capabilities include a wide spectrum of smooth controls, also providing the option to request confirmation for any action by different media (e.g., console).
- Replace your RACF password exit by powerful password quality control. For example, you may apply individual password policies to different kinds of users matching their risk and skill levels – and preventing "post-its" at terminals.
- Perform password quality screening to determine the rules and requirements most of your users struggle with.
- Prevent FTP from weakening your security! Manage FTP security smart that critical data cannot escape and malicious activity becomes impossible.
- Achieve highly precise and granular protection of critical commands and services – "all or nothing" is finally history. E. g. user authentication may be performed by any product as soon as it runs in any authorized mode. With SF-NoEvasion you no longer need to allow any authorized environment to perform authentication for all your user IDs, especially not for your most critical ones. This significantly improves protection of your Web/Java applications available from outside.
- Prevent the use of highly critical but 100% unnecessary commands! For example, there is never a reason why a RACF administrator needs to issue a "SETROPTS NOSAUDIT" command thereby disabling important audit logging.
- Limit authorities depending on time, weekday or presence of other employees.
- Prevent any weaknesses that may be used for professional attacks! The provided attack-and-misuse detection in real-time lets you react instantly, such as by delaying failed logins, resuming revoked user IDs automatically, and more.

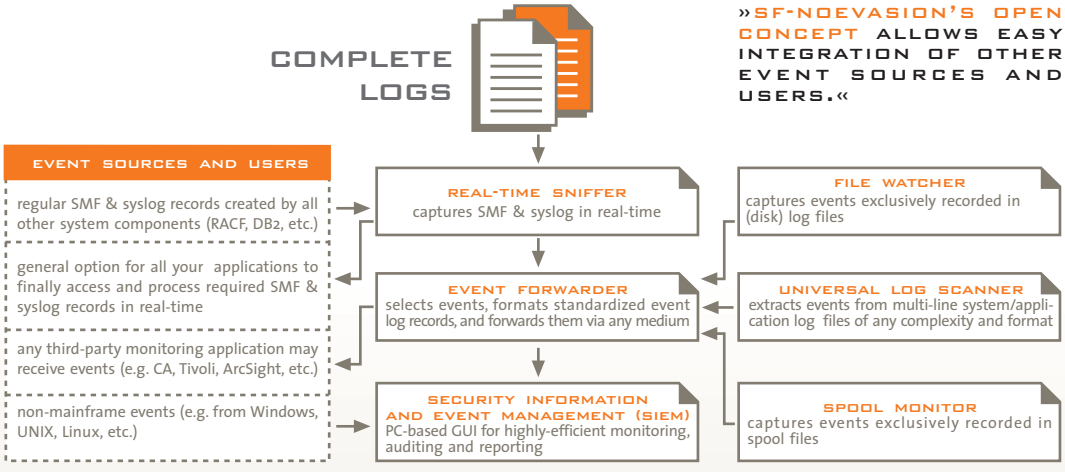
» Compliance via automated modification (completion) of commands and service requests means true relief and efficiency:

- Perform automatic completion (modification) of commands and service calls in order to automatically comply with your policy. This lets you fully automate your compliance controls! E.g., any UACC > READ will be automatically replaced by "UACC (NONE)".
- Prevent the use of the mostly critical PRIVILEGED attribute, which provides free resource access without any logging by the automatic "PRIVILEGED into TRUSTED" conversion.
- Let all users coming via FTP, the Web server or other environments automatically receive the RESTRICTED attribute, and disable all critical privileges.

FURTHER COMPONENTS COMING WITH SF-NOEVASION®

»The "whole truth" is provided in a standardized manner – of course, in real-time!

- SF-NoEvasion provides all its logs in a standardized manner, namely as SMF records. It thus easily becomes part of your regular audit and log procedures.
- A powerful SMF reporting utility is included making all audit and security relevant standard z/OS SMF records also easy to use (e.g., RACF, DB2, TCP/IP etc.).
- The provided plug and play Event Forwarder connects SF-NoEvasion easily to any third-party monitoring solution, such as SIEMs, IDS and others (e.g. CA, Tivoli, ArcSight, etc.) – any medium is supported (e.g. syslog, etc.).



»SF-NOEVASION'S OPEN CONCEPT ALLOWS EASY INTEGRATION OF OTHER EVENT SOURCES AND USERS.«

WWW.FEDTKE.COM » TEL. ++800-DRFEDTKE (WORLDWIDE TOLL-FREE) » ++800-37333853