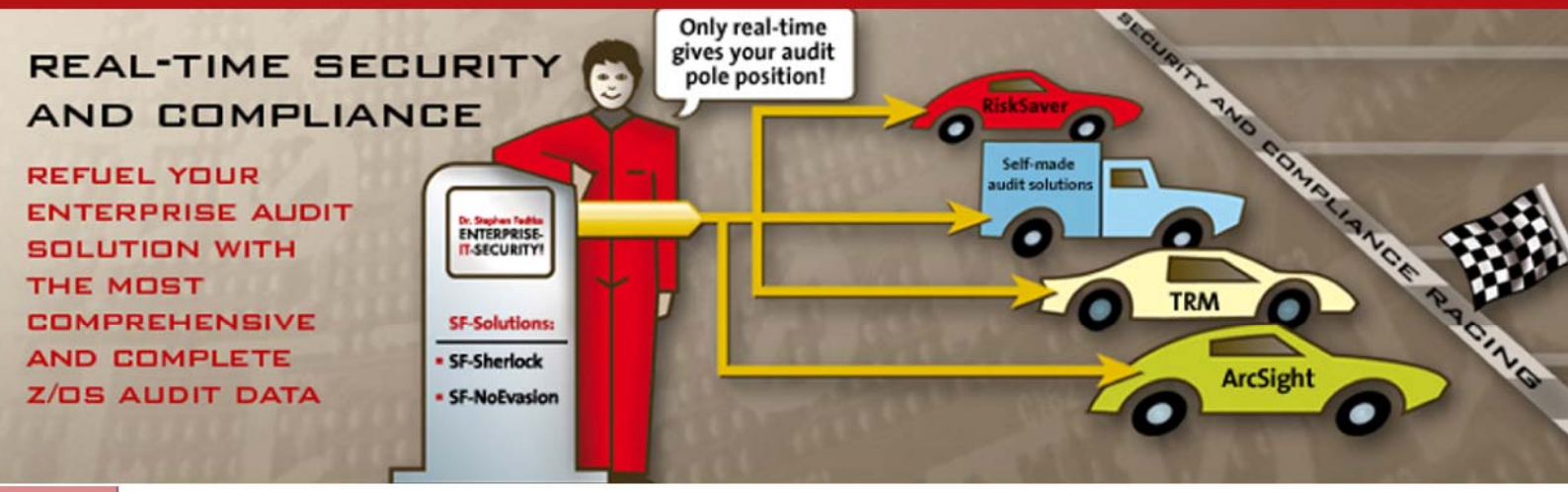
SIEM MAINFRAME (Z/OS) INTEGRATION

10 IMPORTANT REASONS WHY STANDARD CONNECTORS ARE SIMPLY INSUFFICIENT



10 important reasons why your SIEM‘s standard z/OS mainframe connectors do not match today’s demands on security, compliance and fraud prevention

1. **z/OS mainframe events do not reach your SIEM in real-time**, and “show up” too late for proper correlation.
2. **Critical z/OS events are not limited to RACF and DB2,** but also come from TCP/IP, Crypto, and much more.
3. **Risk of completely missing events.** Some critical activity never becomes logged by the z/OS operating or security systems and thus will never reach your SIEM. For example, authorized software may suppress auditing on its own discretion (e.g. authentications/logins), exclude system commands from the syslog, and much more.
4. **Risk of improperly or insufficiently logged events.** Even if activity principally becomes logged, some z/OS audit records do not provide all details required for proper transparency. For example, password changes are logged on such a mediocre level of clearness by RACF, also some system commands, and others.
5. **Comprehensive mainframe-specific know-how is necessary** in order to properly select, classify and priorize all archive, correlation, fraud and compliance-relevant events. Mainframes are servers of high complexity, and corresponding vulnerabilities and attack patterns differ significantly from UNIX, Linux, Windows, etc.
6. **Mission-critical applications and products create their own individual SMF records.** Corresponding events will never reach your SIEM via RACF SMF or syslog records. Typical examples are Beta92, Beta93, etc.
7. **Event log sources on the mainframe are not limited to SMF and syslog,** but may also come from locations that are even harder to “tap” - especially if event delivery in real-time is required. For example, most z/OS applications and daemons write important SIEM-relevant events into spool files, or MVS and USS log files, etc.
8. **Your SIEM’s correlation rules require knowledge on privileged users, sensitive resources, and critical operations from a mainframe’s perspective.** Since original z/OS log data, such as SMF and syslog records, does only partially provide these essential classifications, you need to enrich (tag) events on your own. Improper classification questions your correlation’s quality and power by **causing false positives and similar artifacts.**
9. **Neither completeness assurance nor (malicious) event suppression prevention measures** are applied by z/OS. This quality assurance and audit trail hardening is essential for your SIEM to rely on gap-less event data.
10. **Your SIEM’s demand for z/OS events need to be configurable completely independent** from the regular audit data created by the mainframe teams, and may especially not enlarge the required storage and CPU time.

But there is also good news! In case your z/OS mainframe requires a SIEM connection on more than an “alibi level” you no longer need to accept 10 pitfalls accompanying standard connectors. Your mainframe platform is simply too important, and your SIEM investment was too high for ending just with a “final disposal site” of useless logs. **With SF-NoEvasion you have the economically high efficient option to employ the most powerful audit and compliance data provider** that comprehensively **feeds your SIEM in real-time** to finally achieve top-level security and compliance combined with powerful correlation.

Additional information:

- SF-NoEvasion provides plug & play connectors for major leading SIEM solutions, such as ArcSight, RSA enVision, and more. Refer to the “news” section at **www.enterprise-it-security.com** to determine their current certification status, or simply contact us via phone or e-mail.
- More information on SF-NoEvasion, and how it assists you achieving today’s required levels of compliance, resulting from PCI, Basel II or III, ISO, SOX, FERC, DOD, HiPAA, etc., is provided by our download and forum sections at **www.enterprise-it-security.com**
- The

  http://www.fedtke.com/feed_your_SIEM_properly.htm

  link provides you direct access to the **SF-NoEvasion product flyer**.
- The above given 10 strong reasons still remain valid in case your mainframe runs with CA-ACF2 or CA-TSS instead of RACF. SF-NoEvasion supports RACF as well as CA-ACF2 and CA-TSS.

Contact:

Dr. Stephen Fedtke
System Software
Seestrasse 3a
CH-6300 Zug
Switzerland
Tel. ++41-(0)41-710-4005
Fax. ++41-(0)41-710-4008
www.enterprise-it-security.com