SF-RISKSAVER®

ENTERPRISE AUDIT CONSOLE (SEAC)

YOUR GOALS

JUST-IN-TIME, EFFICIENT AND COMPLETE ENTERPRISE AUDITING VIA AUTOMATION AND CONSOLIDATION

VENDOR-INDEPENDENT AND CROSS-PLATFORM INCIDENT MANAGEMENT

» ONE OF THE MOST INNOVATIVE AUDIT SOLUTIONS FOR ACHIEVING A RISK AND COMPLIANCE MANAGEMENT THAT IS UP-TO-DATE, POWERFUL AND COST-EFFICIENT «

Your company strives for solid and effective real-time risk, security and compliance management for a timely identification and successful defence as well **as achieving a good [risk] rating**.

The current strict legislation and regulations, such as Basel II, KonTraG, IT Baseline Protection Manual (German Federal Office for Information Security), Sarbanes Oxley (SOX), U.S. Department of Defense (DOD) Regulations, Gramm Leach Bliley Act (GLBA), RS FAIT 1, HIPAA Security, 95/46/EC Data Protection Directive and the **certification criteria according to ISO or BS**, among others, require that your company apply precise, efficient and effective measures for risk identification and defence in all IT-based processes.

You regard a **powerful IT and business process auditing** as a crucial measure for successful risk management and understand it as a constantly and widely implemented business process of high importance that brings all the risks together at a central processing point, such as through analysis, rating, decision and reporting.

For an **effective defence against risks that sufficiently complies with legislation and is audit-secure**, you expect a high level of timeliness and completeness from auditing. Despite the complexity and breadth of the topics and processes to be audited, you would like to process each audit incident properly and not only observe them. For you, Auditing comprises both

- **Event monitoring:** rating events and procedures with respect to policy compliance and the ability to detect any suspicious event or activity immediately, **and**
- **Status checking:** examining settings, parameters, configurations, etc. for potential weak spots and vulnerability as well as for policy and regulation compliance.

Aside from setting such high goals and expectations, benchmarking and **general market competition require management with minimal (available) resources** and thus maximum productivity in the audit and related work processes. Therefore, you do not want to question your current investments in security and audit technologies, which exist in the form of logs, tools, policies and the like, but rather keep them productive and profitable. Instead of replacement, you want to consolidate all audit-relevant information sources into a vendor-independent and cross-platform management. Thus, you want **an overall enterprise audit platform** that is open, comprehensive and establishes a central, fully automated, and highly productive audit workflow – also in the context of **ITIL, COBIT, BS7799**, among others.

AUTOMATED ENTERPRISE AUDITING IS THE EFFECTIVE SOLUTION TO THE TECHNICAL AND LEGAL REQUIREMENTS OF TODAY'S RISK MANAGEMENT

PERFORMANCE

INCIDENT AUDITING = EVENT + STATUS AUDITING

REAL-TIME COMPLIANCE MANAGEMENT

INCIDENT NAVIGATOR FOR AN EFFICIENT AND AUTOMATED PROCESSING

COST REDUCTION THROUGH AUDIT CONSOLIDATION AND CENTRALIZATION FOR PROTECTING ALL CURRENT INVESTMENTS IN SECURITY AND AUDITING

LOG CONSOLIDATION

CORRELATION

MAINFRAME SUPPORT

SUITABLE FOR LARGE IT INFRASTRUCTURES

INTRUDER AND INSIDER MONITORING

SUSPICIOUS ACTIVITY DETECTION SYSTEM (SADS) FOR DETECTING EXTRUSION AND OTHER SUSPICIOUS ACTIVITIES

TRANSFORMING THE TECHNICAL DETAILS INTO CLEARLY UNDERSTANDABLE INCIDENTS

SUPPORTING ANY GIVEN COMPANY AND IT ORGANIZATION

IDENTITY MAPPING FOR A TRANSPARENT, COMPREHENSIVE IDENTIFICATION (USER, SYSTEMS, ADDRESSES, ETC.), AND REDUCING COMPLEXITY

INTELLIGENCE MACHINE (SIM)

BUSINESS PROCESS MONITORING

SCORING: SUPPORTING BOTH »MALUS« AND »BONUS« RATING

TRANSFORMS »DATA« INTO »INFORMATION« INTO »GUARANTEED AUDITED, TRANSPARENT INCIDENTS«

POWERFUL REPORTING

OPEN AND GENERALIZED INTERFACES SUPPORT ANY GIVEN AUDIT DATA SOURCES

SQL DATA BASE

INTEGRATED ARCHIVE DATABASE

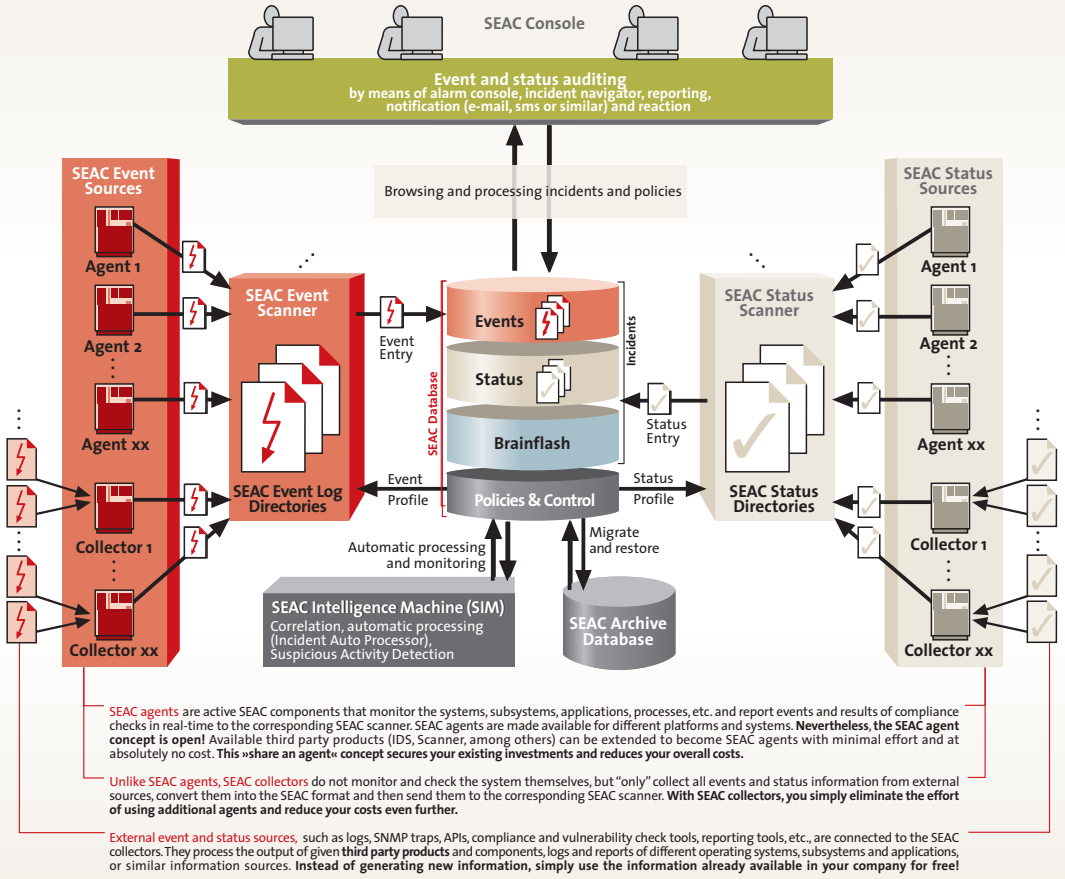
[0-4] ALERT LEVEL MODEL IS PART OF THE STANDARD DELIVERY

ROLE-BASED USER MANAGEMENT AND SUPPORT OF EXTERNAL AUTHENTIFICATION

ALARM CONSOLE WITH A NAVIGATING STRUCTURE

COUPLING TO TICKET, PROBLEM OR OTHER ITIL-RELATED SYSTEMS

AUTOMATIC NOTIFICATION AND REACTION



SEAC agents are active SEAC components that monitor the systems, subsystems, applications, processes, etc. and report events and results of compliance checks in real-time to the corresponding SEAC scanner. SEAC agents are made available for different platforms and systems. **Nevertheless, the SEAC agent concept is open!** Available third party products (IDS, Scanner, among others) can be extended to become SEAC agents with minimal effort and at absolutely no cost. **This »share an agent« concept secures your existing investments and reduces your overall costs.**

Unlike SEAC agents, SEAC collectors do not monitor and check the system themselves, but "only" collect all events and status information from external sources, convert them into the SEAC format and then send them to the corresponding SEAC scanner. **With SEAC collectors, you simply eliminate the effort of using additional agents and reduce your costs even further.**

External event and status sources, such as logs, SNMP traps, APIs, compliance and vulnerability check tools, reporting tools, etc., are connected to the SEAC collectors. They process the output of given **third party products** and components, logs and reports of different operating systems, subsystems and applications, or similar information sources. **Instead of generating new information, simply use the information already available in your company for free!**

SOLUTION: SF-RISKSAVER ENTERPRISE AUDIT CONSOLE (SEAC)

»Demand:___Working together with leading IT installations in the financial and insurance sectors has led to designing and developing the SF-RiskSaver Enterprise Audit Console (SEAC), which is the audit component of the SF-RiskSaver risk management automation solution. High demands in risk management and prevention, as well as the complex structure of audit organizations, have been requirements that helped inspire the highly sophisticated SEAC design, which meets today's technical and legal requirements. SEAC covers both event and status auditing, while its open concept stands for modern and highly efficient enterprise auditing in **risk-sensitive companies**.

»Technology:___Together with its **open, vendor-independent and cross-platform concept**, the Enterprise Audit Console sets up an umbrella over all IT systems, applications and services creating audit-relevant information. Regardless of the format that this information appears in and whether these sources already imply cross-platform aggregations in the sense of a »partial umbrella«, **all your previous investments in security and audit technologies can be integrated and are thus most protected**. You may finally follow the policy: »new tools and agents only when absolutely necessary, since everything is already available«. SEAC is the central, enterprise-wide audit application, which consolidates all of auditing's daily activities in a highly productive, automated workflow – from the moment of incident visualisation to processing and reporting.

»Completeness:___Aside from the ergonomic event and status visualisation in the form of an **»alarm console«**, SEAC's **incident navigator** is a well-designed concept for »processing event and status«. You can distinguish today's audit organizations according to their ways and levels of dealing with reported non-compliant events or settings, namely whether

- events and status checks (compliance checks) »are merely looked at and archived« or examined by way of spot checking, or
- **a current and complete processing of all events and status checks,** including a documentation of the complete auditing process, is performed containing information on each level, starting from the first analysis to subsequent research and the final rating when »closing the case«. The purpose is for auditing to meet today's strict legal requirements by being current, durable and complete while working very effectively, thereby acting as an essential building block to a highly reliable risk and compliance management.

»Success guaranteed:___Particularly in today's financial and insurance sectors, an auditing made by »merely looking through« and »archiving reports« is not sufficient for **protection that is effective and legally exonerates you from risks**. Every relevant audit incident therefore has to be »processed«. Processing both elementary types of audit incidents, event (action, procedure) and status (condition, setting, parameter, configuration) in a modern audit organization has particularly high requirements of **ergonomics and productivity**. The aspect of »minimal processing cost« and the detection of suspicious activity or procedures belong to SEAC's important, unique features. It combines the consistently successful continuation and transition of extremely effective and reliable automation concepts, such as SF Sherlock's »logical traps« and »audit status report«, in an enterprise audit solution that is open, vendor-independent, cross-platform and inter-departmental.

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM