SF-RISKSAVER®

IHR ZIEL

ZEITNAHES, EFFIZIENTES
UND VOLLSTÄNDIGES
ENTERPRISE AUDITING
DURCH AUTOMATION
UND KONSOLIDIERUNG

HERSTELLER- UND
PLATTFORMÜBER-
GREIFENDES
INCIDENT-MANAGEMENT

» EINE DER INNOVATIVSTEN AUDIT-LÖSUNGEN FÜR MODERNES SCHLAGKRÄFTIGES KOSTENEFFIZIENTES RISIKO- UND COMPLIANCE-MANAGEMENT. «

ENTERPRISE AUDIT CONSOLE (SEAC)

Ihr Unternehmen strebt – **auch für ein gutes Rating** – ein **konsequentes und effektives Risiko-, Security- und Compliance-Management** an, um Gefahren rechtzeitig identifizieren und erfolgreich abwehren zu können.

Aktuelle strenge gesetzliche Regelungen, wie Basel II, KonTraG, Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), RS FAIT 1, HIPAA Security, 95/46/EC Data Protection Directive, BSI-Grundschutz, etc. und **Zertifizierungen nach ISO oder BS** fordern von Ihrem Unternehmen präzise und effizient wirksame Massnahmen zur Risiko-Identifikation und -Abwehr in allen IT-basierten Prozessen.

Sie sehen ein **schlagkräftiges IT- und Business-Process-Auditing** als wichtige Massnahme für ein erfolgreiches Risiko-Management an und verstehen es als permanenten wie auch breit angelegten Unternehmensprozess von hoher Wichtigkeit, der die Risiken zum Zweck der Analyse, Bewertung, Entscheidung und Berichterstattung an einen zentralen Punkt der Bearbeitung zusammenführt.

Für eine **juristisch ausreichende, revisionssichere und faktisch wirksame Risiko-Abwehr** erwarten Sie vom Auditing ein hohes Mass an Zeitnähe und »Vollständigkeit« - trotz Komplexität und Breite der zu auditierenden Themen und Abläufe. Aus diesem Grund möchten Sie jeden Audit-Incident wirklich bearbeitet und nicht nur wahrgenommen wissen, und Auditing umfasst für Sie beides,

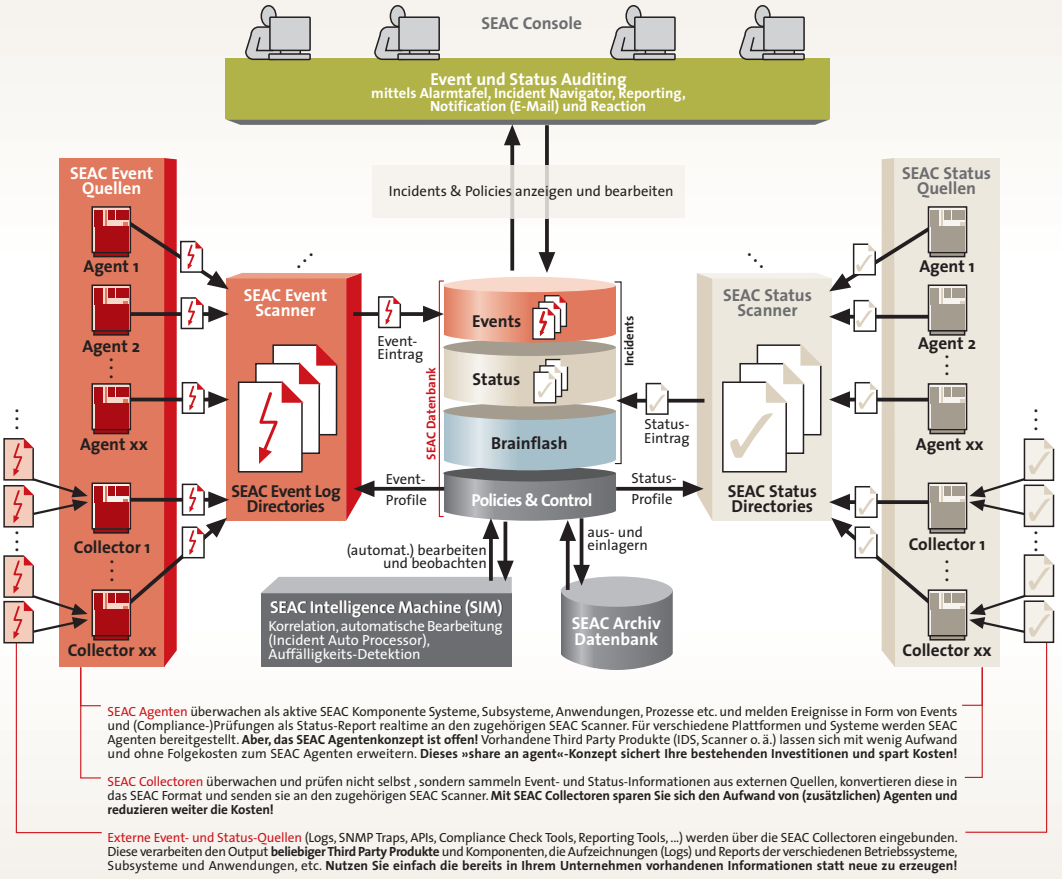
- **Event-Überwachung**, um Ereignisse und Vorgänge hinsichtlich ihrer Zulässigkeit und Auffälligkeit zu bewerten, **und**
- **Status- bzw. Compliance-Checking**, um Zustände, Einstellungen, Parameter, Konfigurationen, etc. auf Ordnungsmässigkeit und potentielle Schwachstellen zu überprüfen.

Kostendruck und der allgemeine Wettbewerb fordern trotz dieser hohen Zielsetzungen und Erwartungen ein **Auskommen mit minimalen - vorhandenen - Ressourcen** und damit eine maximale Produktivität in den Audit-(Arbeits-)Prozessen. Sie möchten deshalb die bestehenden Investitionen in Security- und Audit-Technologien in Form vorhandener Logs, Tools etc. nicht – erneut – in Frage stellen, ablösen oder redundant ergänzen, sondern weiter produktiv ausschöpfen bzw. schützen und im Sinne einer **Audit-Konsolidierung** alle vorhandenen Audit-relevanten Informationsquellen **hersteller- und plattformübergreifend** in eine zentrale, automatisierte, hochproduktive Enterprise-Audit-Gesamtoberfläche zusammenführen - z.B. auch im Rahmen von **ITIL, COBIT, BS7799** o.ä.

AUTOMATISIERTES ENTERPRISE AUDITING ALS WIRKSAME ANTWORT AUF DIE HEUTIGEN TECHNISCHEN UND JURISTISCHEN ANFORDERUNGEN DES RISIKO-MANAGEMENTS

LEISTUNG

- INCIDENT AUDITING = EVENT + STATUS AUDITING
- COMPLIANCE-MANAGEMENT
- INCIDENT-NAVIGATOR FÜR EINE EFFIZIENTE UND AUTOMATISIERTE BEARBEITUNG
- AUDIT-KONSOLIDIERUNG UND -ZENTRALISIERUNG ZUM SCHUTZ DER BESTEHENDEN SECURITY- UND AUDIT-INVESTITION
- LOG-KONSOLIDIERUNG
- KORRELATION
- MAINFRAME-UNTERSTÜTZUNG
- INTRUDER AND INSIDER MONITORING
- SUSPICIOUS ACTIVITY DETECTION SYSTEM (SADS) ZUR AUFFÄLLIGKEITS- UND EXTRUSION-DETEKTION
- UMWANDLUNG DER TECHNISCHEN DETAILS IN VERSTÄNDLICHE INCIDENTS
- UNTERSTÜTZUNG BELIEBIGER ORGANISATIONSFORMEN
- IDENTITY MAPPING FÜR EINE TRANSPARENTE ÜBERGREIFENDE IDENTIFIKATION (USER, SYSTEME, ADRESSEN ETC.) UND ZUR KOMPLEXITÄTSREDUKTION
- INTELLIGENCE MACHINE (SIM)
- BUSINESS PROCESS MONITORING
- KENNZAHLENSYSTEME MIT MALUS- UND BONUS-SCORING
- TRANSFORMIERT »DATEN« IN »INFORMATIONEN« IN »(GARANTIERT) AUDITIERTE VERSTÄNDLICHE INCIDENTS«
- LEISTUNGSSTARKES REPORTING
- OFFENE SCHNITTSTELLEN ERLAUBEN BELIEBIGE AUDIT-DATEN-QUELLEN
- SQL-BASIERTE DATENHALTUNG
- EIGENES ARCHIV
- [0-4]-ALERT-LEVEL-MODELL IST TEIL DER STANDARD-AUSLIEFERUNG
- EIGENES USER-MANAGEMENT UND OFFENE AUTHENTIFIZIERUNGSSCHNITTSTELLE
- ALARM-TAFEL MIT EXPLORER-ÄHNLICHER STRUKTUR
- KOPPLUNG AN TICKET-, PROBLEM- ODER ANDERE ITIL-SYSTEME MÖGLICH
- AUTOMATISCHE BENACHRICHTIGUNG UND REAKTION



SEAC Agenten überwachen als aktive SEAC Komponente Systeme, Subsysteme, Anwendungen, Prozesse etc. und melden Ereignisse in Form von Events und (Compliance-)Prüfungen als Status-Report realtime an den zugehörigen SEAC Scanner. Für verschiedene Plattformen und Systeme werden SEAC Agenten bereitgestellt. **Aber, das SEAC Agentenkonzept ist offen!** Vorhandene Third Party Produkte (IDS, Scanner o. ä.) lassen sich mit wenig Aufwand und ohne Folgekosten zum SEAC Agenten erweitern. **Dieses »share an agent«-Konzept sichert Ihre bestehenden Investitionen und spart Kosten!**

SEAC Collectoren überwachen und prüfen nicht selbst , sondern sammeln Event- und Status-Informationen aus externen Quellen, konvertieren diese in das SEAC Format und senden sie an den zugehörigen SEAC Scanner. **Mit SEAC Collectoren sparen Sie sich den Aufwand von (zusätzlichen) Agenten und reduzieren weiter die Kosten!**

Externe Event- und Status-Quellen (Logs, SNMP Traps, APIs, Compliance Check Tools, Reporting Tools, ...) werden über die SEAC Collectoren eingebunden. Diese verarbeiten den Output **beliebiger Third Party Produkte** und Komponenten, die Aufzeichnungen (Logs) und Reports der verschiedenen Betriebssysteme, Subsysteme und Anwendungen, etc. **Nutzen Sie einfach die bereits in Ihrem Unternehmen vorhandenen Informationen statt neue zu erzeugen!**

LÖSUNG: SF-RISKSAVER ENTERPISE AUDIT CONSOLE (SEAC)

»Bedarf:___In Kooperation mit grossen IT-Anwendern im Finanz- und Versicherungssektor entstand die Audit-Komponente der Risiko-Management-Automationslösung SF-RiskSaver, die Enterprise Audit Console, kurz SEAC. Die hohen Ansprüche in punkto Risiko-Management und –Vorsorge sowie die komplexe Struktur ihrer Audit-Organisationen waren Vorlage für eine optimale Ausrichtung der SEAC am heutigen technischen und juristischen Bedarf der Praxis. Die SEAC deckt beide Bereiche ab, Event- und Status-Auditing, und steht für modernes zeitgemäßes sowie effizientes Enterprise Auditing in **sicherheitssensiblen und risikobewussten Unternehmen.**

»Technologie:___Die Enterprise Audit Console bildet mit ihrem **offenen, herstellerunabhängigen und plattformübergreifenden Ansatz** ein Dach über alle Systeme, Anwendungen und Dienste innerhalb der IT, die audit-relevante Informationen bereitstellen. Gleichgültig in welchem Format diese Informationen vorliegen und auch unabhängig davon, ob diese Quellen – im Sinne eines »Teil-Daches« – bereits übergreifende Zusammenfassungen vornehmen. **Sämtliche Ihrer bereits getroffenen Investitionen in Security- und Audit-Technologien werden eingebunden und sind deshalb bestens geschützt** – das Motto lautet »neue Tools und Agenten nur wenn unbedingt nötig, denn eigentlich ist schon alles vorhanden«. Die SEAC ist damit die übergreifende zentrale Anwendung, in der das Auditing seine täglichen Aktivitäten in einen hochproduktiven automatisierten Arbeitsprozess zusammenführt, von der Visualisierung (Anzeige) über die Bearbeitung bis hin zum Reporting.

»Ganzheitlichkeit:___Zentrales Merkmal der SEAC ist neben der ergonomischen Event- und Status-Visualisierung in Form einer ampelähnlichen **»Alarm-Tafel«** der konzeptionelle Rahmen um die »Bearbeitung von Event und Status« über den **Incident-Navigator**. Heutige Audit-Organisationen lassen sich im Umgang mit gemeldeten Ereignissen bzw. fehlerhaften Einstellungen/Zuständen danach unterscheiden, ob

- Events und Status-Prüfungen (Compliance-Checks) »nur gesichtet und abgelegt« bzw. stichprobenartig untersucht werden, oder
- **eine zeitnahe und vollständige Bearbeitung aller Events und Status-Prüfungen** einschließlich einer Dokumentation des gesamten Auditierungsprozesses erfolgt; von der ersten Analyse über die Nachforschungen bis zur Abschlussbewertung »des Falls«. Ziel ist, durch Zeitnähe, Nachhaltigkeit und Vollständigkeit das Auditing den strengen heutigen gesetzlichen Anforderungen gerecht und als Baustein des Risiko- und Compliance-Managements besonders wirksam werden zu lassen.

»Erfolgsgaranten:___Insbesondere im Finanz- und Versicherungsbereich reicht heute ein Auditing durch »bloße Sichtung« und »Ablage der Reports« für eine **wirksame und juristisch entlastende Risiko-Vorsorge** nicht aus; es wird daher jeder relevante Audit-Incident »bearbeitet«. Die Bearbeitung der beiden elementaren Audit-Incidents, Event (Ereignis, Vorgang) und Status (Zustand, Einstellung, Parameter, Konfiguration), in einer modernen Audit-Organisation stellt deshalb besonders hohe Anforderungen bezüglich **Ergonomie und Produktivität**. Der Aspekt »kostenminimale Bearbeitung« und die Funktionalität zur »Auffälligkeits-Detektion« gehören aus diesem Grund mit zu den wichtigen Alleinstellungsmerkmalen der SEAC. Sie verkörpert die konsequente erfolgreiche Fort- und Umsetzung der äußerst wirksamen und sich in der Praxis bewährten Automationskonzepte »logische Falle« und »Audit-Status-Report« von SF-Sherlock in eine hersteller-, plattform- und abteilungsübergreifende Enterprise Audit-Lösung.

Dr. Stephen Fedtke
ENTERPRISE-IT-SECURITY.COM