

# Managed Security Information Management

Mehr Effizienz, Sicherheit und Compliance für Ihre IT



Suchen Sie Unregelmäßigkeiten im Netzwerkverkehr Ihres Unternehmens wie die Nadel im Heuhaufen?

Dann ist Managed Security Information Management die richtige Lösung für Sie.

## Vorteile auf einen Blick

- » Zentrale Sammlung aller wichtigen Ereignisse relevanter IT-Systeme
- » Korrelation der Ereignisse zeigt unerkannte Zusammenhänge auf
- » Plattformübergreifende Fehlersuche
- » Erkennung von Angriffen und schnelle, konsolidierte Alarmierung
- » Minimierte Reaktionszeiten auf sicherheitsrelevante Vorfälle
- » Einsparung von bis zu 15 Prozent des Personalaufwands zur Fehleranalyse in der IT-Infrastruktur
- » Umsetzung von Compliance-Anforderungen

## Komplexität reduzieren

Spätestens seit der Entwicklung des TCO-Modells durch Bill Kirwin von Gartner im Jahre 1987 weiß die IT-Branche, dass die Betriebskosten von IT-Komponenten deren Anschaffungskosten in der Regel um ein Vielfaches übersteigen. Was auf den ersten Blick erschrecken mag, hat auch seine guten Seiten. Denn es bedeutet, dass eine Senkung der Betriebskosten ein Vielfaches des hart erkämpften Einkaufsrabatts einspart.

In Zeiten steigenden Kostendrucks ist daher die Senkung der IT-Betriebskosten ein wirksamer Hebel für Unternehmen, um bei knappen Budgets mehr Spielraum für geschäftsfördernde Investitionen zu schaffen.

Je größer und komplexer eine IT-Infrastruktur ist, desto aufwändiger gestaltet sich ihr Betrieb. Und umso schwieriger wird es, die Wirkung einzelner Informationen auf das Ganze zu erkennen. Denn wenn Ursache und Wirkung nicht in einem direkten Zusammenhang stehen, kann die Suche danach zu einer personalintensiven Angelegenheit werden. So führt fast jedes IT-System zwar ein Protokoll aller wichtigen Ereignisse, die dort stattgefunden haben. Doch die Log-Daten aller Systeme einzeln händisch zu analysieren und miteinander in Zusammenhang zu bringen, ist entweder ein

sehr zeitaufwändiges Unterfangen oder ab einer gewissen Zahl an Systemen faktisch kaum möglich. Aus diesem Grund haben wir für unsere Kunden das Managed Security Information Management – kurz Managed SIM – entwickelt.

### **Konsolidieren, analysieren, komprimieren**

Der erste Schritt zu mehr Transparenz, Effizienz und Sicherheit in der IT eines Unternehmens besteht darin, die wichtigen Ereignismeldungen aller relevanten IT-Systeme an einer zentralen Stelle zusammenzuführen. Zu diesem Zweck stellen wir unseren Kunden eine Vielzahl vorkonfigurierter Kollektoren zur Sammlung der Log-Daten aus ihren Anwendungen, Netzwerkkomponenten, Sicherheitsprodukten und Betriebssystemen zur Verfügung. Ist für eine Datenquelle, wie beispielsweise eine selbst entwickelte Anwendung, kein Kollektor verfügbar, schreiben unsere Spezialisten nach einem Audit der Anwendung bei Bedarf dafür einen individuellen Kollektor.

Diese Kollektoren sammeln dann zunächst alle Ereignismeldungen der ihnen zugewiesenen Systeme ein. Anschließend entfernen sie Dubletten, normalisieren die Meldungen und senden sie

komprimiert an unsere zentrale Korrelations-Engine. Durch diese mehrstufige Architektur ist einerseits die Skalierbarkeit des Managed-SIM-Service gewährleistet und andererseits für eine optimale Bandbreitennutzung auf den Weitverkehrsstrecken gesorgt. Wir überwachen dabei kontinuierlich die Funktionsfähigkeit der Kollektoren bei unseren Kunden und sorgen zeitnah für alle erforderlichen Updates.

Alles was Sie für den Einstieg in das Managed SIM benötigen, ist eine IP-Verbindung von den Kollektoren in unser Entrance-Netz. Um den Rest kümmern sich unsere Spezialisten.

### 15 Prozent Effizienzgewinn bei der Fehlersuche

In unseren hochverfügbaren und abgesicherten Rechenzentren korrelieren und analysieren leistungsstarke Appliances schließlich alle einlaufenden Daten und ziehen dabei externe Zusatzinformationen wie beispielsweise den Symantec DeepSight Information Service hinzu. Dann vergleichen sie die gewonnenen Erkenntnisse mit den bei ihnen hinterlegten Regeln und lösen gegebenenfalls entsprechende Prozesse aus. Diese zentrale Analyse der unternehmensweiten Systemereignisse lässt sich dabei zu den verschiedensten Zwecken vorteilhaft nutzen.

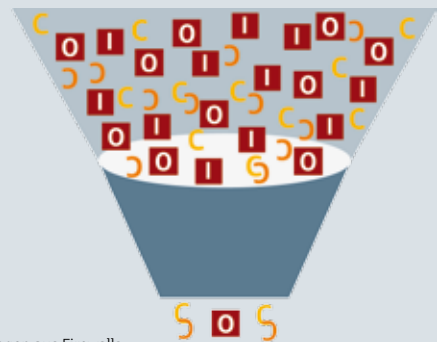
Mit entsprechend hinterlegten Richtlinien kann das Managed SIM durch die zentrale Sicht auf sämtliche Ereignisse aller Komponenten beispielsweise Ursachen von Netzwerkproblemen in kürzester Zeit erkennen und dem Administrator in einem von ihm generierten Bericht aufzeigen.

Die Praxis hat dabei gezeigt, dass sich so bis zu 15 Prozent Effektivitätsgewinn bei der Fehleranalyse erzielen lassen.

### Compliance verbessern

Netflow-Daten aus Routern liefern Informationen über Verbindungen im Netzwerk. Integriert man auch diese Daten in das Managed SIM, lassen sich damit beispielsweise interne Richtlinien in Bezug auf Datenströme überwachen sowie Unregel-

Das Managed SIM erfasst und kombiniert alle Statusmeldungen und sorgt damit für Transparenz



Statusmeldungen aus Firewalls  
 Statusmeldungen der Intrusion Detection Systeme und Anwendungen

mäßigkeiten im Netzwerkverkehr frühzeitig erkennen. Dies ist ein zentraler Bestandteil eines umfassenden Policy Compliance Managements, das Unternehmen dabei unterstützt, die Anforderungen von Euro-SOX, dem Payment Card Industry Data Security Standard (PCI), Basel II oder dem „Sicheren IT-Betrieb“ des Informatikzentrums der Sparkassen-Organisation (SIZ) zu erfüllen.

### Unbegrenzte Möglichkeiten

Dies sind nur drei Anwendungsszenarien, in denen das Managed SIM durch die zentrale Sicht auf alle Systemereignisse Unternehmen einen Mehrwert bietet. Mit Hilfe von benutzerdefinierten Abfragen und Berichten sowie gemeinsam mit unseren IT-Spezialisten generierten Korrelationsregeln lassen sich beliebig viele weitere Analysen durchführen. Die Grenzen setzt hier allein die Phantasie.

## Über Finanz Informatik Technologie Service (FI-TS)

FI-TS ist ein Tochterunternehmen der Finanz Informatik (FI) und hat sich seit 1994 als einer der führenden IT-Servicepartner der Finanzbranche etabliert. Der Outsourcing-Anbieter überzeugt durch langjährige Erfahrung, Branchenkompetenz, Technologie-Know-how und Beratungsexpertise. Maßgeschneiderte Dienstleistungen optimieren die IT-Kosten, machen Banken und Finanzdienstleister noch effizienter und bieten so konkrete Wettbewerbsvorteile. Die Erfüllung aktueller Governance-Anforderungen sowie die konsequente Umsetzung moderner Sicherheits- und Qualitätsanforderungen sind für FI-TS selbstverständlich. FI-TS beschäftigt in Deutschland am Hauptsitz in Haar

bei München und an den Standorten Hannover, Nürnberg und Offenbach rund 520 Mitarbeiter. Das Unternehmen erwirtschaftet einen Gesamtumsatz von circa 128 Millionen Euro – davon mehr als 70 Prozent non captive. Zu den namhaften Kunden, die sich auf die kompetenten Services von FI-TS verlassen zählen unter anderem BayernLB, Landesbank Hessen-Thüringen, DekaBank, Deutsche Kreditbank, Deutsche WertpapierService Bank, Hauck & Aufhäuser, LBS IT, Sparkassen-Finanzportal und die Bank of Scotland.

## IT intelligent nutzen.

Gerne beraten wir Sie ausführlich und stellen mit Ihnen eine auf Ihre Anforderungen abgestimmte Lösung zusammen. Sprechen Sie mit uns.

**Finanz Informatik Technologie Service GmbH & Co. KG**  
Vertrieb · Richard-Reitzner-Allee 8 · 85540 Haar  
Telefon +49 89 94511-8393 · Fax +49 89 94511-8952  
kundenanfrage@f-i-ts.de · [www.f-i-ts.de](http://www.f-i-ts.de)