VitalSigns SIEM Agent for z/OS – Case Studies

Dieser Text ist eine Übersetzung von Kundenreferenzen die Pi-Systemprogrammierungs-GmbH von Software Diversified Services, Inc. erhalten hat. Die englische Version stellen wir gerne zur Verfügung.

HealthCare Case Study: Beispiel für die Einfachheit der VitalSigns SIEM Agent for z/OS Installation

Das IT Management eines großen Krankenhauses mit tausenden von Anwendern und einem in Wochenfrist fälligen Mainframe Security Audit, war besorgt über das was unter der Oberfläche des hauseigenen Mainframe Security Systems gefunden werden könnte. Die Konstellation erlaubte es nicht Zeit in einem aufwendigen Entscheidungsprozess zu verschwenden. Das Management sah sich mit möglichen finanziellen Strafen konfrontiert, sollte sich herausstellen, dass Regierungsauflagen hinsichtlich des Schutzes persönlicher und sensitiver Patienten Daten nicht eingehalten würden. Zusätzlich kam hinzu, dass die aktuellen, täglichen Mainframe Security Audit Prozessen des Absendens von Batch Prozessen, dem Warten auf die Auslieferung der Druckreports, dem Review der Daten, und die Wiederholung des Zyklus für zusätzliche forensische Analysen, einfach nicht funktionierte.

Das Krankenhaus hatte bereits Zeit und Geld in den Betrieb eines Enterprise SIEM Produktes investiert und die Möglichkeiten der Konsolidierung der Mainframe Security Events in den SIEM Server eruiert. Mit der Untersuchung der Software Diversified Serives (SDS), entschloss sich das Management für den Betrieb von SDS VitalSigns SIEM Agent auf dem Mainframe. Aufgrund der bevorstehenden Audit Deadline, wurde VitalSigns ohne üblichen Proof of Concept und Software Trial Tests direkt in Produktion genommen.

Die Produkt Installation auf dem Mainframe erfolgte in weniger als 8 Mann Stunden. In weniger als zwei Tagen, war der Network Security Administrator, ohne vorheriges Mainframe Knowhow in der Lage, das Produkt zu konfigurieren, Policies zu schreiben, Mainframe Security Events zu sammeln, zu analysieren und sie in den SIEM Server mit Firewall- und anderen Open Plattform Security Events zu platzieren.

Die Anzahl zeitraubender Mann Stunden für das Durchschauen von Mainframe Druckreports und ihrer Abhängigkeit zu Lieferergebnissen anderer Abteilungen konnte drastisch reduziert werden. Mit der eingesparten Zeit rücken jetzt andere wichtige Security Themen in den Fokus.

Durch die Inbetriebnahme von SDS VitalSigns SIEM Agent auf dem Mainframe, in Tagen, war das Krankenhaus in der Lage, Mainframe Security Events mit anderen Events aus dem Netzwerk zu konsolidieren. So konnte bereits gekaufter Software zum Durchbruch verholfen werden, manuelle Prozeduren wurden in voll automatische Prozeduren konvertiert und die Anforderungen der Auditoren konnten erfüllt und übertroffen werden.

Pi-Systemprogrammierungs-GmbH Teichstraße 39E D-63225 Langen T: +49 6103 71254 M: +49 171 850 7132 Email: info@pi-sysprog.de

In den Worten des Kunden: "Wir nutzen VitalSigns um das schwierige Problem zu lösen, RACF Logs real time von einer Plattform zu einer anderen zu bekommen. Die Software hilft uns Security Probleme auf unseren Systemen zu entdecken und fehlerfrei in UNIX Syslog Server zu transferieren. Eine sehr nützliche Software!"

Bank Case Study: Beispiel für VitalSigns Software CPU Performance

Viele der VitalSigns Bank Kunden nutzen IBM als “Managed Service Provider” für den Betrieb ihrer Mainframe Umgebungen. Im Rahmen eines Chargeback und Billing Reports für einen ihrer Bank Kunden kam IBM eines Tages auf SDS zu. Die VitalSigns Software, obwohl lizenziert, erschien nicht in dem Report. Fragen wie “läuft die Softwares wirklich?” oder “da ist ein Fehler in der Software” wurden an das SDS Support Team adressiert. Es konnte festgestellt werden, dass die VitalSigns Software korrekt und reibungslos lief. Das Problem dass die VitalSigns Software in den Reporting Systemen nicht angezeigt wurde, lag darin begründet, dass die CPU Usage Reporting Parameter für den Charge-back Report des Kunden zu hoch angesetzt waren.

Zusammengefasst, in allen 27 aktiven LPAR’s, verbrauchte die VitalSigns Software weniger CPU Power als die Bank im Vergleich zu anderen Software Produkten hatte und die CPU Verbrauchs Parameter wurden heruntergesetzt, so dass IBM die Kosten korrekt an den Bank Kunden berechnen konnte.

Bank Case Study: Beispiel von SDS’s Reaktionsbereitschaft gegenüber Kunden

SDS stellte einem potentiellen Bank Kunden Software für einen Trial zur Verfügung. Der potenzielle Kunde erklärte sich bereit nach Beendigung des Trials die Software zu erwerben, unter der Bedingung dass SDS eine Methode zur Verarbeitung von CICS Applikations Daten auf dem Mainframe bereitstellen würde. SDS akzeptierte diese Herausforderung um den Kundenauftrag zu gewinnen und entwickelte das VitalSigns CICS API (Application Programming Interface). Das VitalSigns SIEM Agent for z/OS CICS API wurde in einer zwei Wochen Periode designed, entwickelt, getestet und vom Kunden abgenommen.

Das VitalSigns SIEM Agent for z/OS CICS API wurde als Resultat einer potentiellen Kundenanforderung in die Basis VitalSigns SIEM Agent for z/OS Software integriert.

Details finden Sie unter folgendem Link (Link VSA) oder sprechen Sie uns an:
Enrico Rammo, Mobil +49-160-1538384 oder enrico@pi-sysprog.de