

Warum VitalSigns SIEM Agent for z/OS

Lt. Analysten wie Gartner führt die Notwendigkeit der Früherkennung zielgerichteter Attacken und Datenverletzungen zum Wachstum neuer & bestehender SIEM Umgebungen. Hierbei planen fortgeschrittene Anwender SIEM Erweiterungen mit fortgeschrittener Profilierung und Analytik. In verteilten Umgebungen ist Security Information & Management Software (SIEM) bereits zum de facto Standard in dem \$1,7 Mrd. großen Markt geworden. Die Marktführer mit Real-time Lösungen sind IBM QRadar, HP ArcSight, Splunk, LogRhythm und Intel/McAfee.

Aktuell werden z/OS Events nicht für SIEM Server in verteilten Umgebungen zur Verfügung gestellt. Vielmehr werden in z/OS Mainframe Umgebungen folgende Praktiken angewandt:

- Review von Mainframe Logs durch Batch Jobs
- Bestenfalls Analyse am Folgetag
- RACF Review durch Mainframe Security Personal
- DB2 Review durch DB2 System Administratoren

Zwischen Mainframe und verteilter Umgebung herrscht ein klarer Medienbruch, real time in der verteilten Welt und bestenfalls near time in der Mainframe Welt. Das entspricht bei den RAS (Reliability, Availability, Sustainability) Systemen doch eher dem was sich hinter dem US amerikanischen Slogan „Fox guarding the hen house“ und/oder „trust but verify“ verbirgt und das obwohl die Unterlassung Compliance Auflagen nachzukommen, harte Strafen gegenüber Unternehmen, persönliche Schuldverhältnisse und Geldstrafen für Manager und massiven Vertrauensverlust bei Konsumenten bedeutet.

Die Lösung dieses Dilemmas bietet VitalSigns SIEM Agent for z/OS (VSA) dem bereits 2007 patentierten z/OS SIEM Agenten, einem voll umfänglichen Log Consolidation & Compliance Software Agenten, der mit marktführenden SIEM Servern in offenen Umgebungen integriert ist.

Compliance Mandaten unterstellte Industrien wie Gesundheitswesen, Finanzwirtschaft, Versicherungen, Handel und Öffentliche Verwaltung sind betroffen sofern sie z/OS Mainframes betreiben und CIO, CISO, SIEM Projekt Manager und z/OS Compliance Evangelisten dieser Unternehmen sollten Software Diversified Services' VitalSigns SIEM Agent for z/OS Agenten (VSA) evaluieren.

Pi-Systemprogrammierungs-GmbH ist Repräsentant und Distributor für VitalSigns SIEM Agenten for z/OS der US amerikanischen Software Diversified Services, Inc. mit Sitz in Minneapolis, MN. In dieser Funktion vertreiben und supporten wir VitalSigns SIEM Agent for z/OS (VSA) in Europa.

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