LogApp 2.2 verfügbar

iQSol veröffentlicht neue Version der SIEM-Lösung LogApp

Oed-Oehling, 05. März 2013. Die iQSol GmbH hat die neue Version ihrer Sicherheitslösung LogApp veröffentlicht. LogApp ist ein Log-Archivierungssystem und eine Security Information & Event Management-Lösung (SIEM). Die neue Version 2.2 wurde um Windows File Integrity Monitoring und einen Enterprise Reporting Server erweitert. Des Weiteren hat iQSol ihren Alert Messaging Server integriert, ein Enterprise-Alarmierungssystem für Administratoren.

LogApp 2.2 unterstützt hashbasiertes File Integrity Monitoring. Neue, modifizierte und gelöschte Dateien werden dabei anhand von haschbasierten Vergleichen identifiziert und gemeldet. Über Black- und Whitelisting lassen sich punktgenaue Überwachungslisten erstellen. Die Überwachung kann täglich oder zu bestimmten Wochentagen durchgeführt werden. Hashbasiertes File Integrity Monitoring ist unter anderem PCI-kompliant.

Mit dem Enterprise Reporting Server stehen den Administratoren ab sofort alle Möglichkeiten des MS SQL Reporting Services für ein umfangreiches und detailliertes Reporting zur Verfügung. Vorgefertigte Reports gewährleisten ein schnelles Basis-Reporting. Kundenspezifisches Reports können jederzeit ergänzt und bestehende Reports an die konkreten Berichtsanforderungen angepasst werden.

Durch die Überarbeitung der Archivierung konnte die Performance wesentlich verbessert werden. Die nächtliche Archivierung sorgt für eine Reduktion der Datenmenge auf ein benutzerfreundliches Maß.

LogApp 2.2 ist als Appliance-Lösung oder als virtuelle Maschine auf VMWare und Hyper-V sowie als App für Android und iOS erhältlich.

Über LogApp

Die Appliance-Lösung LogApp sammelt alle Events von Windows- und Linuxsystemen sowie Netzwerkgeräten und wertet diese aus. LogApp arbeitet dabei mit Agents und erkennt die Zusammenhänge in Echtzeit. Die Agents können Syslog-Nachrichten von Netzwerkgeräten aller Art entgegennehmen und senden diese an die LogApp weiter. Mit HoneyApps stehen drei verschiedene Honeypotdienste als zusätzliche Datenquelle zur Verfügung. Im Fall eines Angriffs oder Virus im internen Netzwerk werden so zuverlässig Events an die LogApp gesendet. Die Correlation-Engine der LogApp analysiert alle eingehenden Events und erzeugt bei Sicherheitsvorfällen einen Alarm. Die Korrelation kann auf Basis von anpassbaren Regeln oder auch vollautomatisch erfolgen. Alle Events, die die LogAgents und HoneyApps registrieren,

werden unverzüglich auf der LogApp oder auf einem angebundenen Netzwerkshare manipulationssicher archiviert.

Bei akuten Vorfällen ist ein sicherer und schnellstmöglicher Informationsfluss ein entscheidender Faktor, der mit dem Alert Messaging Server sichergestellt wird. Der Alert Messaging Server ist ein vollständig anpassbares Enterprise-Alarmierungssystem für Administratoren in Hochverfügbarkeitsumgebungen. Im Störungsfall wird die zuständige Technikergruppe sekundenschnell benachrichtigt. In Kombination mit einer umfangreichen Monitoring-Lösung kann der Alert Messaging Server systemrelevante Alarme via E-Mail, SMS und Voice-Anruf aussenden.

Weitere Informationen zu den beiden Lösungen unter
http://www.iqsol.biz/de/produkte/.

Über die iQSol GmbH

iQSol ist ein unabhängiger Hersteller für Lösungen im Bereich Unternehmensalarmierung sowie Log-Management. Die SIEM-Lösung LogApp schließt die Lücke im Bereich Log-Archivierung, Log-Management und Event-Korrelierung in Echtzeit. Mit dem von iQSol entwickelten Honeypot-Modul werden Unternehmen bestens vor Trojanern und Bot-Systemen geschützt. Die Spezialisten von iQSol haben langjährige Erfahrungen aus vielen IT-Audits und verfügen über umfassende Kenntnisse gängiger Systems- und Security-Management-Lösungen. Weitere Informationen unter www.iqsol.biz/.

Pressekontakt:
saalto Agentur und Redaktion GmbH | Büro Berlin
Alin Frädrich
Ohlauer Straße 43
D-10999 Berlin
Telefon: +49 30/61657167
E-Mail: alin@saalto.de
www.saalto.de