EVENTSENTRY

IT vorwärts treiben –
mit unübertroffener Einsicht in Ihre Netzwerkdaten.

IT Teams benötigen relevante Netzwerkdaten in Echtzeit um die richtigen Entscheidungen zu treffen - sowohl kurz- als auch langfristig. EventSentry ist eine leicht zu installierende, hoch verfügbare und skalierbare Überwachungslösung welche die Performance, Compliance und Sicherheit in Ihrem Netzwerk verbessert - mit einem unübertroffen Preis-Leistungs-Verhältnis. Durch eine reibungslose und umfassende Überwachung werden Katastrophen verhindert und Kosten gespart. Neue Benutzer können sich in kurzer Zeit mit EventSentry vertraut machen und die leistungsstarke Überwachungslösung problemlos an Ihre spezielle Umgebung anpassen.

SCHLÜSSELFUNKTIONEN:

- Korrelation und Überwachung von Ereignisprotokollen und Logdateien in Echtzeit; Überwachung von Leistungsdaten, Festplattenspeicher, Diensten, Prozessen und mehr auf physikalischen und virtuellen (Cloud) Servern und Arbeitsstationen.
- Verfolgt alle Änderungen an Active Directory™ Objekten und Gruppenrichtlinien. Unterstützt Benutzerstatusberichte und Email-Erinnerung bei Passwortablauf.
- Verfolgen von Prozessen, Konsolen- und Netzwerkanmeldungen, Dateizugriffe, Konten- und Richtlinienänderungen für Regelwerke inkl. GDPR, ISO & PCI.
- Datenvisualisierung mit modernen, aufschlussreichen Dashboards und leistungsfähigen Reportingmöglichkeiten. Das mandantenfähige Reporting basiert auf modernen Web-Technologien und unterstützt eine detaillierte Rechtevergabe.
- Einfache Integration von Kernfunktionen mittels existierender oder neuer Skripte in die Überwachungsumgebung.

KUNDENEMPFEHLUNGEN:

"EventSentry wurde schnell ein essentielles Instrument für die Überwachung von kritischen Infrastruktursystemen."

"Das Schweizer Taschenmesser von Netzwerküberwachungslösungen!!"

"Skaliert weit besser als konkurrierende Lösungen."

"Einwandfreie Kundenbetreuung!"

"Installierung und funktionsfähig in Minuten!"

"Geht weit über Ereignisprotokollüberwachung hinaus."

"Funktioniert genau so wie erwartet."

"Einsicht in unsere Systeme war unglaublich."

Version 5.0

For more information call 312.624.7698
www.eventsentry.com

Features Overview

EVENTSENTRY

Event Log Überwachung & Korrelation
Echtzeitüberwachung und Korrelation des Ereignisprotokolls mit Unterstützung von Schwellenwerten, wiederkehrende Events, Zeitgeber und mehr.

Compliance Tracking (Richtlinieneinhaltung)
Verfolgt und interpretiert Dateizugriffe, Prozessaktivitäten und Konsolenanmeldungen, erfolgreiche und fehlgeschlagene Netzwerkanmeldungen, lokale & globale (AD) Kontoänderungen, um IT bei der Einhaltung von Richtlinien zu unterstützen.

Logdatei & Korrelation
Überwacht jede Art von Logdatei (z.Bsp. IIS, DHCP, Backup, Firewall) in Echtzeit und verschickt Warnmeldungen basierend auf Filterkriterien. Logdateien können im Reporting abgebildet werden.

NetFlow
Visualisiert NetFlow- und sFlow-Verkehr und bietet detaillierte Berichte wie Bandbreitennutzung. Identifiziert Port-Scans und warnt vor bösartigem Netzwerkverkehr. Sysmon Integration korreliert die Prozessnetzwerkaktivität mit NetFlow-Daten.

Umfangreiche Inventarisierung
Inventarisiert installierte Software, Browsererweiterungen, Patches und Hardwareinformationen und virtuelle Maschinen (VMWare© and Hyper-V©). Integriert automatisch mit Hardware Management Tools von Dell© & HP© Servern und zeigt physikalische Ports zu Netzwerk-Switches an.

Umfangreiche Systemüberwachung
Verfolgt alle wichtigen System Metriken wie Festplattenplatz, Performance, Dienste, Neustarts, kritische OS-Dateien und mehr.

Prozesse, Dienste und Scheduled Tasks
Proaktive Überwachung von Diensten, geplanten Aufgaben und Prozessen. EventSentry kann auch Prozesse und Dienste automatisch neu starten.

Zentraler Collector-Dienst
Ein zentraler Kollektordienst unterstützt Komprimierung und TLS Verschlüsselung über unsichere Netzwerke (z.Bsp. Internet). Mobile Clients wie Laptops koennen Daten in lokalem Cache zwischenspeichern.

Sicherheit
Netzwerksicherheit in Echtzeit durch Log-, Datei- (FIM), Dienst- und ARP-Überwachung (erkennt neue Geräte im Netzwerk).

Benachrichtigungen
EventSentry inkludiert 16 verschiedene Benachrichtungstypen, inklusive: SMTP Email, Syslog, SNMP Traps, HTTP(S), Jabber (IM), Datenbank, SNPP, RSS, Textdatei, Prozesse, Reboot, Dienstkontrolle, Desktop und mehr.

Unsichtbare Überwachung
Agents überwachen Server & Workstations mit minimaler Netzwerkauslastung, ohne die Leistung der überwachten Hosts zu beeinträchtigen.

Validationskripte
Sammlung von anpassbaren Skripten welche unsichere Einstellungen, fehlenden Windows Updates/Patches, Compliance-Verletzungen und Fehlkonfigurationen auf überwachten Hosts erkennen.

Web Reporting
Modernes Web Reporting mit Dashboards, Zugangskontrolle, flexibles Reporting, Job-Engine und vielen visuelle Darstellungsmöglichkeiten. Ein umfassendes API ermöglicht den Zugriff auf alle Daten mit Hilfe externer Software. Funktioniert mit allen gängigen Web-Browsern und Mobilgeräten.

Netzwerküberwachung
Zentrale Überwachung von Hosts über ICMP und TCP mit detaillierten Status und Protokoll.

Syslog/SNMP/ARP Daemon
Zentrale Sammlung von sowohl Syslog Nachrichten als auch SNMP Traps (v1-v3) von Unix/Linux Hosts und/oder Netzwerkgeräten. Warnmeldungen können in Abhängigkeit von Filterkriterien in Echtzeit verschickt werden.

FIM: Überwachung der Dateiintegrität
Verfolgt Prüfsummen, Größe, Version, Entropie und digitale Signaturen von kritischen Dateien, um Änderungen zu erkennen und zu verfolgen. Warnmeldungen und Berichte in Echtzeit unterstützen die Einhaltung von diversen Sicherheitsanforderungen.

Version 5.0

For more information call 312.624.7698
www.eventsentry.com