ManageEngine
EventLog Analyzer

EventLog Analyzer ist eine webbasierte Log-Management- und Compliance-Lösung, die Bedrohungen des Unternehmensnetzwerks in Echtzeit erkennt. Die Software unterstützt Unternehmen dabei mit umfangreichen Log-Management-Funktionen, vorkonfigurierten und sofort einsatzbereiten Compliance-Reports und Alarmen, unterschiedlichste Audit-Anforderungen zu erfüllen. Selbst strikte IT-Vorgaben lassen sich so einfacher einhalten als je zuvor.

Features und Vorteile

End-to-End-Log-Management:

Sammeln, analysieren und archivieren Sie Log-Dateien aus über 600 Quellen – inklusive Netzwerkgeräten, Windows- und Linux/Unix-Servern, IBM AS400-Maschinen, Datenbanken, Webservern, Vulnerability Scannern und Threat-Intelligence-Lösungen.

Eventkorrelation in Echtzeit:

Mit den vorkonfigurierten und individuell erweiterbaren Korrelationsregeln können Sie Muster in den protokollierten Log-Files sowie Zusammenhänge zwischen einzelnen Sicherheits-vorfällen erkennen und entsprechend reagieren.

Umfangreiches Anwendungs-Auditing:

Erfahren Sie, wer wann und von wo aus auf welche Daten zugegriffen hat – für alle geschäftskritischen Anwendungen wie IIS- und Apache-Webserver, SQL-Server- und Oracle-Datenbanken.

Bedrohungsanalyse:

Holen Sie sich automatisch die neuesten Informationen aus den STIX/TAXII Threat Feeds und lassen Sie sich in Echtzeit alarmieren, wenn IP- und URL-Adressen mit dem Netzwerk interagieren, die auf der Blacklist stehen.

Incident-Management-System:

Richten Sie sich Alarme ein, die in Echtzeit über Anomalien informieren. Sie können diese Alarme auch automatisch bestimmten Technikern in deren Helpdesk-Software zuweisen.

Integriertes Compliance-Management:

Nutzen Sie vorkonfigurierte Compliance-Reports für IT-Vorschriften wie PCI DSS, FISMA, HIPAA, GLBA, SOX und DSGVO.

Kundenstimmen

Crystal Clear Analytics & Real-time Alerts for Swift Threat Detection

"An order of magnitude reduction in the time necessary to reviewing and analyzing logs. Additionally, ELA provides real-time alerting of significant events. This facilitates rapid analysis and reaction to events. Instead of days before identifying a significant event, the event is known in near real time and can be responded to before it becomes an issue."

Michael Thorp
Principal Information Security Analyst, AAI Corp, Textron, Inc.

Best-in-class Intrusion Detection, Economical Pricing

"Windows event logs and device Syslogs are a real-time synopsis of what's happening on a computer network. EventLog Analyzer is an economical, functional and easy-to-utilize tool that allows me to know what's going on in the network. It's a premium intrusion detection system."

Jim Lloyd
Information Systems Manager, First Mountain Bank

A Scalable Tool Trusted for IT Compliance Demonstration

"Credit Union of Denver has been using EventLog Analyzer for more than 4 years. Provides great value as a network forensic tool and for regulatory due diligence. This product can be rapidly scaled to meet our dynamic business needs. "

Benjamin Shumaker
Vice President of IT/ ISO, Credit Union of Denver

Weitere Vorteile und Features

Agentenbasiertes oder agentenloses Sammeln von Log-Dateien

Indizierung aller durch Menschen lesbaren Log-Formate dank benutzerdefiniertem Log-Parsing

Auditing von Änderungen an kritischen Dateien und Ordnern

Umfangreiche Suchmaschine für forensische Log-Analysen

Intuitive Dashboards und durchdachte Berichte liefern verwertbare Einblicke

www.manageengine.de/eventloganalyzer