Louis Ene

ManageEngine Eventlog Analyzer

Summary

Eventlog Analyzer is presented as a web app used for SIEM within businesses. It works by managing log data that is generated from devices and applications and encrypts it, making it protected within the constraints of forensics and compliance audits. A record of when the data was taken is kept to prove that it hasn’t been tampered with. The analyzer uses a PostgreSQL database by default however this can be changed to either My SQL or MS SQL as the user may prefer one of those. The analyzer can check for file integrity and produce forensic reports for selected logs. The user is also given the ability to import logs remotely through HTTP/S and FTP.

Features

Log Archiving- Logs can be stored to be used as evidence/ references at a later date.

Forensics- The tool can be used in data forensics as overall device access is monitored and can be recorded. Furthermore, log forensics can be used to trace hackers, detect vulnerabilities and aid in disaster recovery.

Log search- EventLog Analyzer can be used to search for logs, assisting in forensics as mentioned above.

SIEM- Overall, this tool is an SIEM tool, meaning that it is designed to manage systems and be used to discover potential threats. Additionally, it is to be used as a point of reference when incidents occur.

MSSP Features- MSSP utilizes security network services. These can include, firewall, VPN and antivirus services.

Notifications (Real-time alerts included)- Users are kept up to date via real-time notifications, allowing problems to be seen immediately and troubleshooting and treatment to begin effective immediately. This is especially necessary as attackers often act very quickly, sometimes finishing an attack before the business even notices.

Compliance Reports- Compliance reports aid in overall governance. This can be used to check how well the business is complying with regulations set for it within the industries that they operate in. Compliance reports are especially necessary for businesses as they help prevent laws being broken and the business receiving any fines.

Log Reports- Log reports offer data that can be used to identify whether or not operations are running smoothly.

Monitoring privileged users- Monitoring users is important as the business can see if there are any suspicious users. However, monitoring privileged users is even more necessary as privileged users often have a lot more access. This means that they can do things on systems that normal users can’t. For example, the finance officer (or similar position) in a company can set the amount of capital that each employee receives monthly through their salary. However, if they are sly enough, they could change their own monthly earnings by increasing it. This is just one of many examples of how privileged users can potentially affect business finances and operations.

Event dating- Key dates are given to events so that they may be traced and archived on the system. The business could use event dating to find patterns within events such as hacker attacks to identify how frequently or around which months/days attacks happen.

Benefits

EventLog Analyzer has many benefits in comparison to other similar SIEM tools. Some of these include how fast it can be setup, it’s easy log management and its ability to be integrated within the workplace

EventLog Analyzer can be setup in under thirty minutes. If the user has any issues with this process, MachineEngine’s official website can be used to help troubleshoot and guide the user through the setup. This ensures that the software can be used and easily learnt by new and inexperienced users in addition to having an already intuitive user interface.

The software itself is a standard SIEM system, meaning that any already-implemented systems don’t have to be reconfigured as the software can be used with hundreds of devices from a range of places.

Most features are easily navigable as the user interface is so intuitive. This has been achieved by the incorporation of a gui set in place of the dashboard, meaning that icons are used for simplicity.

In terms of compliance and industry regulations, the software comes with already existing reports such as ISO 27001 and others like FISMA. As aforementioned, monitoring can be done across the board. Some specific examples of these include privileged users being monitored and login attempts. The software also comes with its own filters whereby the user can generate reports that fit certain parameters.

Logs can be collected with ease and be deciphered, and any updates/alerts can be observed accurately as they happen with the creation, access, deletion and any alterations done to files within the framework.

The management of network threats can be performed fluently as a result of event correlation within the software. Areas of correlation can be spotted instantaneously due to it being real-time. This means that it is made simpler to spot where attacks are coming form, especially if there are any threats form people within the business.

Customer Support

Customer support can be accessed by the user via telephone communications or through ManageEngine’s online support network.

Pricing

EventLog can be used through a free trial at the start, however the user must contact ManageEngine to receive a quote for their software price.

Specifications

EventLog can be used on iOS or on the desktop. On a 32 bit system, the minimum hardware requirements are:

-1ghz, 32 bit Pentium Dual Core processor or equivalent

-2 Gb RAM

-5 Gb HDD available space

For a 64 bit system:

-2.80 ghz, 64 bit (x64) Xeon LV processor or equivalent

-2 Gb RAM

-5 Gb HDD available spac

-Web browser such as Google Chrome, Edge or Firefox

Installation

EventLog Analyzer is installed via the following:

Enter email to start free trial

A computer screen shot of a person holding a book

Description automatically generated

Run the setup



Start the application

A screenshot of a computer screen

Description automatically generated

Enter username/password

A screenshot of a computer

Description automatically generated

Add all devices/everything you want to monitor.

A screenshot of a computer

Description automatically generated