Simplifying Network Security & Log Management

- Monitor Privileged User
- Combat External Threats
- Mitigate Internal Threats
- File Integrity Monitoring
- Conduct Forensic Analysis
- Compliance Management

"The best thing, I like about the application, is the well structured GUI and the automated reports. This is a great help for network engineers to monitor all the devices in a single dashboard. The canned reports are a clever piece of work"

-Senior Network Engineer, Citadel

www.eventloganalyzer.com http://demo.eventloganalyzer.com eventlog-support@manageengine.com

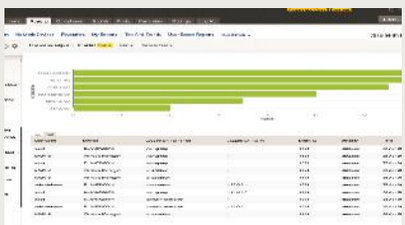
ManageEngine
EventLog Analyzer

Mitigate Internal Security Threat

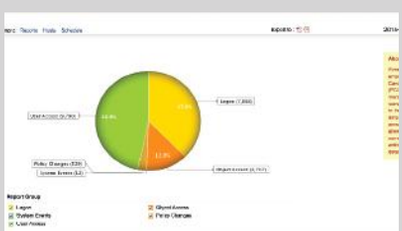
- Conduct user audit trails and monitor privileged user activity with pre-defined user activity and session activity reports.
- Centrally track crucial changes to confidential business data and get a complete audit trail of all the changes that had happened. Get to know in real-time who did what changes and when files and folders are created, modified, accessed, viewed, deleted, and renamed.

Combating External Security Threats

- With 70+ predefined correlation rules detect breach attempts and policy violations.
- Flexible drag-n-drop correlation rule builder allows users to define attack patterns thus helping in proactively reacting to security threats.
- Monitor network for any data breach attempts with 1000+out-of-the-box reports on security auditing, user activity monitoring, account management, threat detection, and file integrity monitoring.
- Quickly neutralize security attacks with real-time SMS/Email alert notifications upon any network anomalies.



Compliance Management

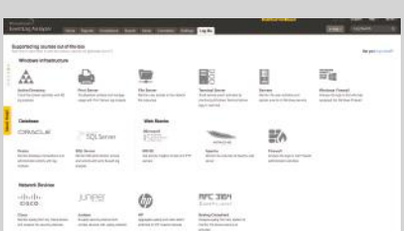


- Generate out-of-the-box reports for various regulatory mandates such as PCI DSS, FISMA, HIPAA, ISO 27001, GLBA, SOX and more.
- EventLog Analyzer provides value added feature that helps creating custom reports for new compliance and thus helps you to meet with growing demands of regulatory mandates.
- Meet log retention requirement of compliance mandate at an ease with secured and tamper proof log archiving techniques.

Forensic Analysis

- Conduct forensic analysis with powerful and efficient search engine that provides wide range of search options including wild card search, phrase search, group search, range search and more.
- Search for anything, not just a handful of pre-indexed fields, and quickly detect network anomalies, misconfigurations, viruses, user activities, system/applications errors, etc. And save the search results as a report or as an alert to mitigate future threats of same kind.

Log Collection



- Supports both agentless and agent based log collection mechanisms
- Collects logs from heterogeneous sources (Windows systems, Unix/Linux systems, Applications, Databases, Routers, Switches and other Syslog devices
- Deciphers any log data regardless of the source and log format
- Allows you to index any machine-generated logs (provided it is in human readable, non-encrypted format) by defining and extracting log file

Download 30 day free trial at www.eventloganalyzer.com/ download.html

www.eventloganalyzer.com eventlog-support@manageengine.com Toll Free : +1 888 720 9500