ZOHO Corp.

Analyzing Logs For Security Information Event Management

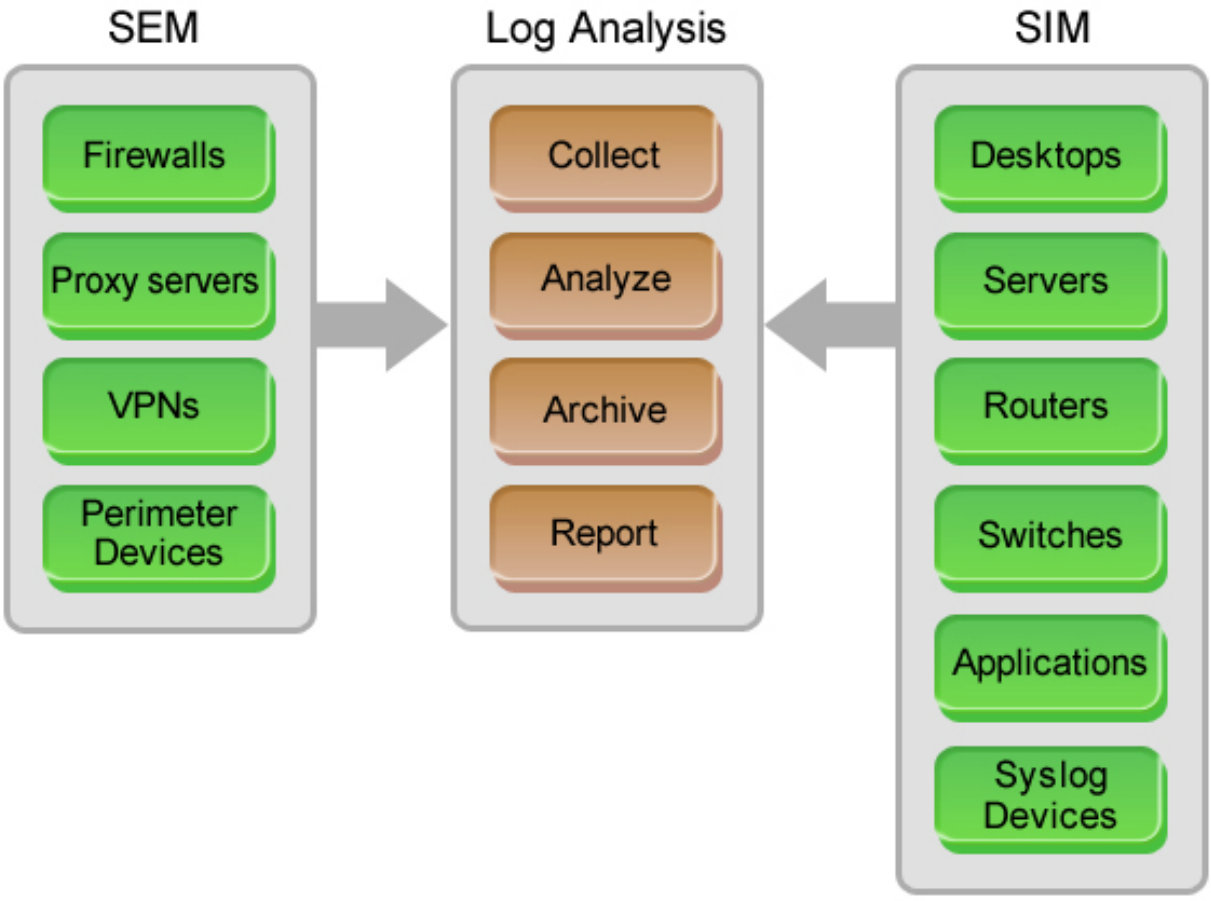
Whitepaper

Importance of Log Analysis

All network systems and devices like Windows/Linux desktops & servers, routers, switches, firewalls, proxy server, VPN, IDS and other network resources generate logs by the second. And these logs contain information of all the system, device, and user activities that took place within these network infrastructures. Log files are important forensic tools for investigating an organizations security posture. Analysis of these log files provide plethora of information on user level activities like logon success or failure, objects access , website visits; system & device level activities like file read, write or delete, host session status, account management, network bandwidth consumed, protocol & traffic distribution; and network security activities like identifying virus or attack signatures and network anomalies.

What is Security Information Event Management?

Security Information Event Management (SIEM) refers to the concept of collecting, archiving, analyzing, correlating, and reporting on information obtained from all the heterogeneous network resources. SIEM technology is an intersection of two closely related technologies, namely the Security Information Management (SIM) and Security Event Management (SEM).



According to Wikipedia "*Security Information Management (SIM), is the industry-specific term in computer security referring to the collection of data (typically log files; e.g. eventlogs) into a central repository for trend analysis. This is a basic introductory mandate in any computer security system. The terminology can easily be mistaken as a reference to the whole aspect of protecting one's infrastructure from any computer security breach. Due to historic reasons of terminology evolution; SIM refers to just the part of information security which consists of discovery of 'bad behavior' by using data collection techniques...*" So, to a large extent SIM is concerned with network systems, like Windows/Linux systems, and applications. As a technology SIM is used by system administrators for internal network threat management and regulatory compliance audits.

SEM on the other hand is concerned with the "real time" activities of network perimeter devices, like firewalls, proxy server, VPN, IDS etc. Security administrators use SEM technology for improving the incident response capabilities of the perimeter/edge devices through network behavioral analysis. The target audience for SEM technology is NOC Administrators, Managed Security Service Providers (MSSP), and of course the Enterprise Security Administrators (ESA).

Introducing ManageEngine® EventLog Analyzer for SIM

ManageEngine® EventLog Analyzer (www.eventloganalyzer.com) is a web-based, agent-less syslog and windows event log management solution for security information management that collects, analyses, archives, and reports on event logs from distributed Windows host and, syslog's from UNIX hosts, Routers & Switches, and other syslog devices. EventLog Analyzer is used for internal threat management & regulatory compliance, like Sarbanes-Oxley, HIPAA, GLBA, PCI, and others.

EventLog Analyzer is used to:

- Provide a centralized repository for all the collected resource logs
- Mine through the collected system logs and generate pre-defined and custom reports
- Zero in on applications causing performance and security problems
- Determine unauthorized access attempts and other policy violations
- Identify trends in user activity, server activity, peak usage times, etc.
- Obtain useful event, trend, compliance and user activity reports
- Understand security risks in your network
- Monitor critical servers exclusively and set alerts
- Understand server and network activity in real-time
- Alert on hosts generating large amounts of log events indicating potential virus activity

- Schedule custom reports to be generated and delivered to your inbox
- Generate reports for regulatory compliance audits
- Identify applications and system hardware that may not be functioning optimally
- Centralized archival of all collected logs for meeting regulatory compliance requirements
- And more…

Introducing ManageEngine® Firewall Analyzer for SEM

ManageEngine® Firewall Analyzer (www.fwanalyzer.com) is a firewall log analysis tool for security event management that collects, analyses, and reports on enterprise-wide firewalls, proxy servers, and VPNs to measure bandwidth usage, manage user/employee internet access, audit traffic, detect network security holes, and improve incident response.

Firewall Analyzer helps you to:

- Manage heterogeneous perimeter devices
- Provide a centralized repository for all the collected device logs
- Mine through the collected device logs and generate pre-defined and custom reports
- Analyze incoming and outgoing traffic/bandwidth patterns
- Identify top Web users, and top websites accessed
- Project trends in user activity and network activity
- Identify potential virus attacks and hack attempts
- Determine bandwidth utilization by host, protocol, and destination
- Detect anomalies through network behavioral analysis
- Analyze efficiency of firewall rules
- Determine the complete security posture of the enterprise
- Provide user specific firewall views to manage authorized perimeter device
- Generate instant reports for bandwidth usage, traffic statistics, user activities, and more
- Manage remote/customer premises firewalls and generate customized reports
- And more…

About ManageEngine.

ManageEngine is the leader in low-cost enterprise IT management software. The ManageEngine suite offers enterprise IT management solutions including Network Management, HelpDesk & ITIL, Bandwidth Monitoring, Application Management, Desktop Management, Security Management, Password Management, Active Directory reporting, and a Managed Services platform. ManageEngine products are easy to install, setup and use and offer extensive support, consultation, and training. More than 30,000 organizations from different verticals, industries, and sizes use ManageEngine to take care of their IT management needs cost effectively. ManageEngine is a division of ZOHO Corporation. For more information, please visit www.manageengine.com.