**Event Log Management and Monitoring**

Computer networks all around the world generate daily records of events occurring in their system. Some events are routine while others indicate potential security breaches or weak network health. **Event log files** consist of log information that can help organizations reduce their exposure against malware, intruders, damages and legal obligations.

This useful **log data** has to be gathered, stored, monitored and managed by enterprises to meet regulatory compliance requirements by standards such as HIPAA, Sarbanes Oxley, GLB, Basel II, PCI DSS, FISMA and NISPOM. This can be quite a tiresome job as log files come in various formats from different sources and in large numbers.

Your network devices and servers produce thousands of system event **log entries** every day. Approximately 95% of your log files record entries of all events or transactions taking place in your system, such as user logins and server crashes. When reviewing logs manually, it is highly unlikely to successfully locate a security or compliance issue.

**Why Central Event Log Monitoring and Management is Important?**

Centralized **Event log management** and monitoring helps you audit, monitor and report every file access, policy changes, unauthorized access by a user or any activity involving breach of personal information such as financial data, employee details or patient records. Centralized event log monitoring includes management of Syslog, Event Logs and W3C logs.

Your operating system has several event logs in need of constant monitoring. One of these is **security log**, which provides information on the logged users and their activity on the network. These logs are important for IT security personnel who know how to read logs and understand any vulnerabilities that exist in implementing security.

**Syslog** is a log transmission standard protocol and is implemented by many networking devices, hardware and software platforms, and Linux and UNIX systems. It provides detailed information on the number of devices and device’s status. This information can help you in getting insight into unusual behavior through variation in performance or operational patterns.

Storing syslog data also helps in ensuring compliance by generating audit logs to trace event logs that are affecting reliability of network and data protection. Likewise, **W3C logs** inform about server and user activity. Event log monitoring of these logs is important as they identify any attempt to compromise your network.

Similarly, other event logs such as information logs, warning logs and error logs provide specific information. For instance, a warning log may not be significant at first, but indicates a potential problem in the future such as low disk space. An **error event** could indicate problems such as service startup failure or loss of data.

**Event Log Management and Monitoring Best Practices**

1. **Define Audit Policy Categories**

Audit Policy simply means the **types of security events** that you need to record in security event logs of workstations and servers. For Windows NT, you need to manually set up the audit policy on individual workstations and servers. For other Windows and Active Directory logs, it can be enabled for entire group of servers.

1. **Automate and Merge Log Records Centrally**

Syslog files and windows event logs are decentralized by default. It means that each system records its own event logs. Administrators with **security and compliance responsibility** should consolidate these records in a central store to carry out log monitoring, analysis and management. Automating records helps meet compliance standards, ensure log data reliability and save time.

1. **Create Real-Time Alert and Notification Policies**

When creating an event log management plan, you need to create certain **policies** on the types of events you need to monitor. Not only that, but all monitored events that give an insight into security, hardware or application issues must have a mechanism to be traced back to their point of origin.

Depending upon organization-specific requirements and flexibility of your event log monitoring solution, define a methodology or policy for **continuous monitoring** of your logs. This should be based on how frequently you need to check logs for required events in real-time. The event log explorer should then generate notification whenever it detects a log of interest.

1. **Generate Reports for all Stakeholders**

As an organization seeking compliance, you must pay attention to reports. Not only does it prove compliance, it also provides important data on **security trends**. Reporting can also help you assess your security measures and change any policies based upon events that can or already resulted in a security breach.

**What Do You Need in an Effective Event Log Management Solution?**

When choosing an **event log monitoring solution**, you need to ask the following questions:

* Is the solution compatible with the event archiving solution?
* What formats are available for generating reports?
* How much of work is done already in the prepackaged event log report that generates?
* Is it easy to recall customized filters for repeat use?
* What data sources are the reports generated from?

You also need to ensure that your event log management and monitoring solution can

* Quickly **Store and Analyze Log Files** for Compliance by collecting, archiving and backing up Windows events, Syslog, or W3C/IIS logs.
* Give alerts to any suspicious activity with continuous real-time monitoring
* Automate the log monitoring and management process and save time and effort spent on manual tasks
* Consolidate all the event logs into a central database
* Analyze logs and quickly detect security threats or any unauthorized activities
* Monitor, alert and report access or permission changes to folders, files or objects.
* Identify potential threats by collecting common log types such as **Microsoft events, Syslog or W3C/IIS logs**
* Protect outside access to critical information such as financial data, employee credentials, business data or patient information

**Virtual Metric’s Event Log Management and Monitoring**

Virtual Metric’s Event log management and monitoring solution provides **detailed analysis of events** in your infrastructure. Our smart alerts keep you updated with potential threats and issues in your network. Our Log Analytics suite collects and analyzes event logs and presents them on a single user-friendly dashboard.

Click [here](https://www.virtualmetric.com/analytics) to get a free trial and find out more about our event log management solution.