FEATURE

Log Management Is A Vital Security Arsenal for IT Admin

Log Management solutions help administration gain better insights into security threats and meet regulatory compliance requirements by monitoring and analyzing log data from the network infrastructure

BY GEETHA NANDIKOTKUR

The fact that the network security solutions market as per IDC is in excess of $100 million in India, with a compounded annual growth rate of close to 18 per cent over the last few years explains the critical nature of data that the network has absorbed. This underscores the fact that IT infrastructure is the backbone of an organisation, and is made up of network devices, systems and business-critical applications that generate high volumes of log data every day. Criminals, who are becoming more skilled by the minute, have their eyes on this invaluable data in order to get access to confidential corporate data. With such a high volume of data, it is impossible for IT administrators to meet IT security requirements by manually analysing the log data.

Sridhar Iyengar, VP--Product Management, ManageEngine lays emphasis

on the need for automation which requires a comprehensive log management and compliance reporting software to keep information security threats at bay. It would not be an overstatement to say that an effective log management SIEM solution could be a security arsenal for IT administrators.

Iyengar is of the opinion that the network infrastructure is always prone to risk as customers deploy different products and varied applications used across the infrastructure, as also cloud and other emerging solutions that bring their set of security challenges. All these are escalating the challenges for the administrator and increasing the vulnerability of data.

Challenges in Log Management

Some of the key challenges that enterprises face with regard to log management which Iyengar has listed out are:

- Analysing logs for relevant security intelligence--which means analysing information in real time from terabytes of log data--is the greatest challenge that network administrators face, besides manual analysis and correlation of log data for IT security, which is difficult and prone to human error
- Centralising log collection--collecting log data from heterogeneous sources at a central place can be a daunting task for IT administrators
- Meeting IT Compliance Requirements--IT administrators want compliance auditors to finish their work with minimal effort; and verbal assurance to compliance auditors is never sufficient
- Conducting effective root cause analysis--searching through logs to find the root cause of a network problem or spotting a pattern in events is like finding a needle in a haystack. IT administrators find it very difficult to get answers to their questions when they need them the most
- Making log data more meaningful--network administrators need better data representation in different graphical formats, reports and dashboards
- Tracking suspicious user behavior data thefts, outages and system crashes can be caused by the most trusted employees and users who have privileged access to business-critical applications, devices, systems, and files
- Archiving logs centrally--is a mandate for all enterprises to meet compliance requirements. Log archiving depends on the policies laid down by the enterprise and the regulatory compliance it follows. The log archiving period varies according to the compliance audit.

Why should IT admin turn to SIEM Log Management tool?

Iyengar recommends that IT administrators define their own security policy for internal and external employees based on the Security Information and Event Management (SIEM) solutions.

One important aspect that Iyengar emphasises on is deploying solutions that are easy to deploy, and more flexible and scalable, with no army of consultants needed to implement them

"Organisations need tools that can derive meaningful, actionable information, and security intelligence from the log data," says Iyengar and further explains, "Monitoring and analysing log data is not a one-time process that will secure your network. It should be an ongoing process in which the log data is collected, monitored, and analysed in real time at a central location."

Some of the key Log management solutions that are most sought after, according to Iyengar, include these:

a) SIEM tools for log collection that have the capability to aggregate logs from heterogeneous sources; the advantage of the universal log collection feature is that enterprises will be able to collect and analyse any log data format from any source.

b) Log analysis is a key element and the log analyser solution which helps in analysing raw log data and generating intelligence for IT security in real time should be the core of any SIEM solution.

c) User Monitoring, the most important tool as most major data breaches have happened because organisations have failed to monitor the activities of their users, especially users who have privileged rights.

d) File Integrity Monitoring, a tool that helps thwart data breaches and meet stringent compliance requirements observed by enterprises.

e) Dashboards drive SIEM solutions and help IT administrators take timely action and make the right decisions during network anomalies.

"Security data must be presented in a very intuitive and user-friendly manner. The dashboard must be fully customisable so that IT administrators can add and view only the security information they need," avers Iyengar. ITNEXT

Key Benefits

- Rapid RoI in making effective use of the log data and automate the entire process of log management, enabling IT administrators to provide top-notch IT security in a short span of time.
- With an SIEM solution in place, IT administrators will find time to invest more on strategic IT than in manually managing their log data.
- Real-time monitoring and provides powerful insights and network security intelligence into user behaviors
- SIEM solutions unite all critical IT security capabilities such as compliance reporting, file integrity monitoring, user monitoring, device monitoring, etc
- Maintenance cost in multiple log management and analysis point products is totally eradicated with single SIEM tool

Find more at online on the website
www.itnext.in/resources/articles