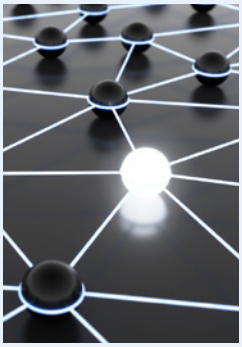
OPTIMIZING

Security Information and Event Management System

The Problem

Integrated Security Information and Event Management (SIEM) solutions are widely deployed to protect networks from internal and external threats and comply with a variety of data protection regulations. Large firms and institutions invest significant financial and personnel resources to implement and maintain SIEM systems but often overlook the most fundamental element of these systems, log management. SIEM solutions provide a dizzying array of charts, graphs and dashboards based on sophisticated event correlation analysis, but these analyses are only as good as the data collected from network devices and applications.



Data Integrity

Many SIEM solutions focus on data analytics rather than reliable log message transfer and storage. To ensure the integrity of log messages, a SIEM system should transfer logs via an encrypted channel and store them in an encrypted format. For data to be used in legal proceedings following a forensics investigation, log messages must be stored in tamper-proof, encrypted format with a timestamp and digital signature. Many SIEM solutions do not provide this level of data protection leaving valuable data inadmissible in court.

Performance

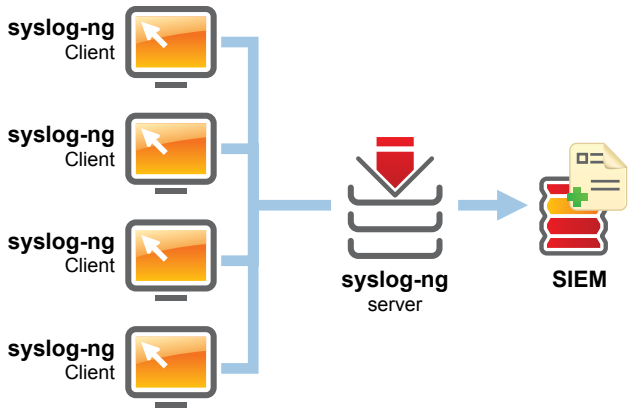
Large networks produce massive amounts of system logs from a wide variety of devices and applications. However, the stream of log messages is not uniformly distributed across time as network loads will fluctuate over the course of the day. IT organizations often purchase SIEM solutions based on peak load requirements which can be an expensive proposition as many SIEM vendors offer usage based licenses or capacity-limited hardware.

THE SOLUTION

How does an organization ensure data security and increase SIEM system performance to optimize Total Cost of Ownership (TCO)? Implement a robust log management infrastructure.

Data Integrity

The Premium Edition of syslog-ng can store log messages securely in encrypted, compressed, indexed, and timestamped binary files, so any sensitive data is available only for authorized personnel who have the appropriate encryption key. The logstore files can be encrypted with multiple encryption keys as well. Timestamps can be requested from external timestamping authorities.



In order to ensure that log messages are not lost due to a broken connection or equipment failure, the log management infrastructure needs to provide a fail-over solution. The Premium Edition of syslog-ng stores messages on the local hard disk if the central log server or the network connection becomes unavailable. The syslog-ng application automatically sends the stored messages to the server when the connection is reestablished, in the same order the messages were received. The disk buffer is persistent – no messages are lost even if syslog-ng is restarted or terminates unexpectedly.

Performance

Centralized Log Collection

Centralized log management is essential to SIEM system performance. The log messages from numerous network devices such as servers, routers, and firewalls and a wide variety of applications ranging from ERP solutions to server OS software need to be collected and stored so that SIEM systems can transform potentially millions of syslogs into real-time, actionable information about network operation and security. The syslog-ng Premium Edition application supports over 50 platforms including a wide variety of Linux, UNIX, HP, IBM, Microsoft Windows, and Solaris variations.

Variable Rate Message Flow-Control

Controlling the flow of system logs being sent to a SIEM system allows IT organizations to leverage their investments in data analytics systems by investing for average rather than peak capacity. Flow-control uses a control window to determine if there is free space in the output buffer of syslog-ng for new messages. If the output buffer is full, then the destination cannot accept new messages for some reason: for example, it is overloaded, or the network connection becomes unavailable. In such cases, syslog-ng stops reading messages from the source until some messages have been successfully sent to the destination.

Log Classification and Filtering

Depending on the configuration, syslog-ng can receive more than 650,000 log messages per second. Moreover, syslog-ng can manage and classify log messages so that the sophisticated data analytics only process logs relevant to security events making the most of the money invested in SIEM solutions.

LEARN MORE

BalaBit IT Security is an innovative information security company, a global leader in the development of privileged activity monitoring, trusted logging and proxy-based gateway technologies to help protect customers against internal and external threats and meet security and compliance regulations. As an active member of the open source community, we provide solutions to a uniquely wide range of both open source and proprietary platforms, even for the most complex and heterogeneous IT systems across physical, virtual and cloud environments.

BalaBit is also known as “the syslog-ng company”, based on the company’s flagship product, the open source log server application, which is used by more than 650,000 companies worldwide and became the globally acknowledged de-facto industry standard.

BalaBit, the second fastest-growing IT Security company in the Central European region according to the Deloitte Technology Fast 50 (2010) list, has local offices in France, Germany, Italy, Russia, and in the USA, and cooperates with partners worldwide. Our R&D and global support centers are located in Hungary, Europe.

- Read more about BalaBit syslog-ng products
- Request evaluation version
- Request callback