ManageEngine
Log360

DATASHEET

Data collection in Log360

Log360, ManageEngine's comprehensive security information and event management (SIEM) solution, collects and analyzes logs to gain important, actionable security information about various events taking place in the network. This information aids the security team in detecting security breaches or malicious activities in the network efficiently.

Data collection in Log360

• Log360's out-of-the-box support for multiple log formats

One of the major challenges users face while using a SIEM solution is the lack of out-of-the-box support for analyzing different log formats. Log360 can collect, parse, and analyze logs from over 750 log sources, including Windows systems, database platforms, firewalls, intrusion detection systems (IDS) or intrusion prevention systems (IPS), Unix or Linux systems, routers, switches, web servers, and more.

• Ability to configure log sources in one go

Another big challenge in SIEM deployment is configuring the solution to collect log data. Manually adding all the devices and applications in the network for monitoring is a tedious job; Log360 makes it effortless by automatically discovering all the devices that are a part of the user's domain, and listing them for the user to select. Log360 also has the capability to discover and monitor syslog devices based on the **IP range** (Start IP to End IP) or **CIDR range** as specified by the user.

• Log360's data collection methods

Log360 offers two different modes of log collection—agent-based and agentless. Organizations can choose the mode of log collection based on their requirements.

Agent-based log collection

In this technique, an agent is installed in the network to collect log data from a single device or multiple devices, and sends them to Log360 for further analysis. This method can be chosen if users want to collect data from a secured or restricted network, or if there's an internal security policy that doesn't allow direct communication between the device and Log360's log management server. Agents can also be employed in large networks, as they have the capability to reduce bandwidth utilization and enhance the data collection process.

Agentless log collection

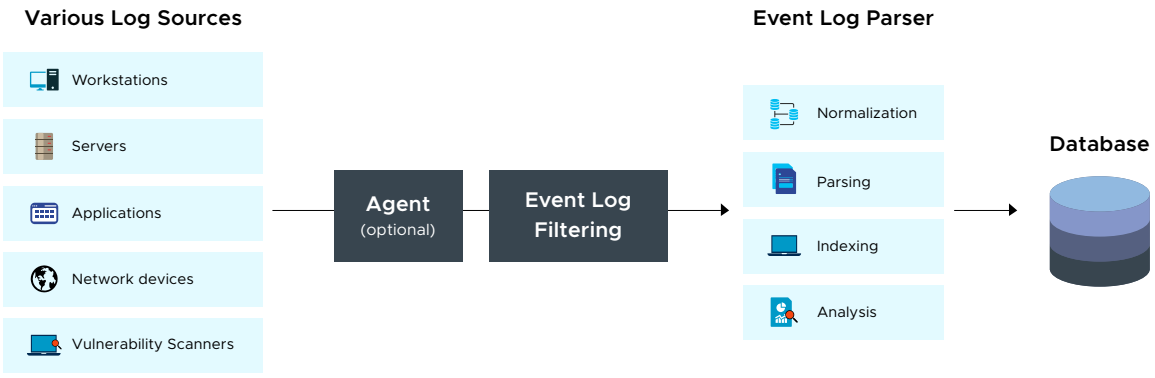
Chosen by most organizations, this technique is easy to configure and employed as the default log collection method by Log360. In this method, Log360 listens to the log data received on specific ports using protocols like Windows Management Instrumentation (WMI).

Log import capability

Log360 allows the user to automatically import log data at specific intervals from local or remote machines using HTTP, File Transfer Protocol (FTP), or SSH FTP. After importing, users can view the name of the device from which the logs were imported, the IP address, protocol, scan time, status of import, as well as the monitoring interval on Log360's console. Additionally, this feature also enables them to schedule the import of log files.

• Secure transmission of log data

To ensure that the security and integrity of event log data is preserved during the log collection and transmission process, Log360 employs various data security techniques. Transmission Control Protocol (TCP), WMI/DCOM, TLS, and HTTPS are some communication protocols are used for the secure and reliable transmission of collected event log data to Log360's log management server. Encryption techniques such as AES-256 and SHA-256 are used to encrypt the data transmitted.



• Parsing and normalization in Log360

Log360 has a built-in log parser to normalize, parse, and index event logs. All the logs that are collected from various sources are normalized to a common format so they can be analyzed and correlated effectively. Log360's log parser breaks down logs into different pieces of information that can be grouped into appropriate sections. The logs are then analyzed for generating reports and alerts that can assist the security team in detecting any cyberthreats in the network.

• Log360's custom log parser:

Apart from providing out-of-the-box support for more than 750 log sources, Log360 can also parse human-readable logs generated by any device or application in the user's network. Manually generating new patterns to index new fields for parsing can get pretty complicated; using Log360's flexible custom log parser, the user can simplify the process to just a few clicks. Users can use the built-in log fields or create custom fields to gain insights by extracting more information.

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats.

Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

ManageEngine
Log360

$ Get Quote

Download