ManageEngine
Log360

SOLUTION BRIEF

Using Log360 to **detect malicious traffic inflow**

www.manageengine.com/log-management

Using Log360 to detect malicious traffic inflow

Monitoring the traffic on your network is essential if you want to keep attackers at bay, and ensure your organization runs smoothly and efficiently. In this age of cyber conflict, threat intelligence and network traffic monitoring tools help organizations protect their sensitive data. Information obtained from these tools can be used in IT use cases to detect security vulnerabilities, troubleshoot network issues, and analyze the impact of new applications on the network.

Without proper network monitoring and threat detecting measures in place, your organization's IT infrastructure will eventually be challenged by detrimental actions that might even be irreversible. To help organizations monitor and detect malicious traffic, ManageEngine Log360 provides various capabilities, including a global threat intelligence database that contains more than 600 million blocklisted IP addresses, URLs, and domain information for detecting and blocking malicious actors.

Let's explore the different threat intelligence capabilities of Log360 that organizations can deploy to detect malicious traffic, prevent attacks, and automatically mitigate them, as necessary.

Detecting malicious traffic with advanced threat intelligence

- **In-depth insights:** Log360's advanced threat intelligence capability provides helpful granular data. Let's say a malicious IP is detected. Log360 enables you to view details including the domain name of the originating IP address, number of times it was flagged on the threat list, its reputation score, and so on. You can also view geolocation information of a particular malicious entity. These details enable you to modify your firewall configuration and block communication relating to unfamiliar locations.

- **Support from numerous threat formats:** Log360 gathers and processes threat feeds from different formats, including STIX, TAXII, and AlienVault OTX.

- **Real-time alerts to thwart malicious intrusions:** Log360 provides instant alerts through emails and SMS when a malicious IP interacts with your network.

- **Detecting entire attack pattern:** Log360's correlation engine can connect the log message with the threat database to detect intrusions and data exfiltration with a malicious source.

  This way, you can quickly and efficiently prevent any compromise in your network security.

Using Log360 to analyze threats in-depth

Log360's Advanced Threat Analytics add-on provides a dedicated built-in tab that lists all malicious IPs, URLs, and domains that have been detected. With this capability you can:

- View the geolocation of malicious entities, and modify your firewall configurations based on the information received, to block communication from unfamiliar locations.
- Associate a reputation score to every threat, and classify it as a high-risk threat if the reputation score is high.
- Categorize the threat based on risk level, and inspect the threat feed data, including the first and last time the threat was detected, and the number of times it was detected.
- Evaluate ways to address a malicious source. Using this capability, IT admins can prioritize sources based on severity level, and develop a course of action to remediate and mitigate the issue.

Gartner's Peer Insights Voice of the Customer 2023 is out!

ManageEngine named a Customers' Choice for SIEM

Check out why

Latest Gartner Magic Quadrant for SIEM is out!

ManageEngine recognized in Gartner's Magic Quadrant for Security Information and Event Management, 2020.

Get the report

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