ManageEngine
Log360

USE CASE

Using Log360 to detect malware

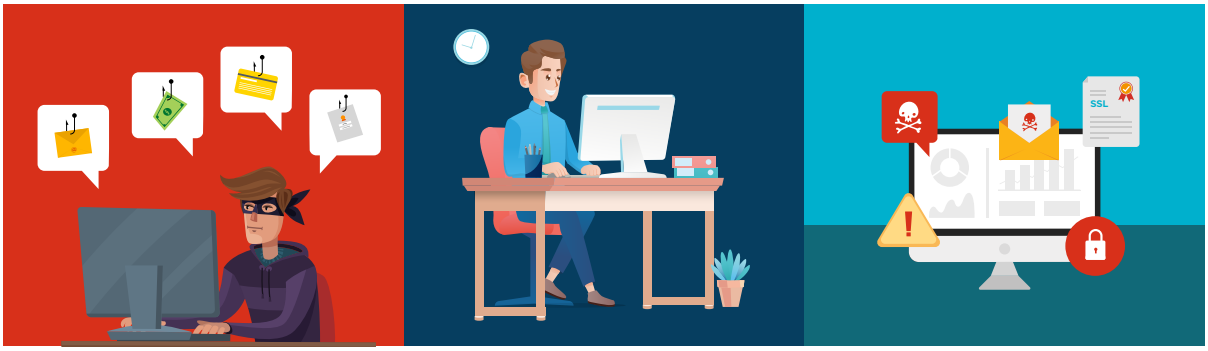
Using Log360 to detect malware

Malware attacks continue to plague enterprises year after year. According to a study by Statista, the total number of new malware detections worldwide amounted to 677.66 million programs as of March 2020.

Combating malware begins with detecting it. Malware such as ransomware and adware immediately encrypts your system files and streams ads. Others like Trojans and spyware are notoriously undetectable. Viruses and worms might operate stealthily until they result in deleted files, sudden shut downs, high disk usage, and even hardware faults.

Given that malware attacks rapidly evolve, how can you ensure the malware detection system in your network is effectively combating this dynamic threat?

How malware works?



1. Malware is delivered to your system via:

- Spam emails
- Vulnerabilities
- Malicious links
- Network propagation

2. It is installed on your system with or without action from the user

3. Possible consequences:

- Encrypts the system
- Steals or manipulates data
- Establishes backdoors
- Steals credentials, bank passwords, and more

While deploying an anti-malware solution is highly effective, it may not be enough, as it wouldn't give you a holistic security view of your network. Further, anti-malware may not take into account factors like account compromise, which can sometimes precede a legitimate software installation that's actually malicious.

This is why you need a security information and event management (SIEM) solution that can correlate events. Building a strong event log correlation and analysis system helps you take proactive steps against malware attacks.

How Log360 can detect malware

Log360, a comprehensive yet easy-to-use SIEM solution, can help you detect and stop malware attacks.

Rule-based correlation engine to detect malware

Log360, a comprehensive yet simple to use SIEM solution, comes with a powerful correlation engine that lets you set rules to identify suspicious patterns in your incoming network logs. With a slew of built-in rules, Log360 correlates various events, and alerts you about suspicious software installations, suspicious service installations, and more.

Behavioral-analytics to detect malware

Log360 takes various factors into consideration before flagging a software installation as malicious. This is possible with behavior analytics performed by the Log360 UEBA add-on, which detects anomalies based on time, count, and pattern. This effectively eliminates false alarms, which is a major challenge in threat detection.

Incident investigation with Log360

Log360 doesn't stop with just malware detection; it also helps in effective investigation and mitigation. Once flagged, you can easily investigate the incident with Log360's correlation reports. The detailed incident timeline and security analytics reports present you with log information that serves as evidence for the security incident.

Log360's end-to-end incident management system comes with a built-in ticketing module that helps assign tickets to security admins, track their status, and ensure accountability in the incident resolution process. This system also has an automatic remediation framework that can associate workflow profiles with correlation rules. These workflow profiles can be executed automatically when the correlation alert is triggered to instantly remediate the incident.

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