ManageEngine
Log360

DATASHEET

THE RULE-BASED, REAL-TIME CORRELATION ENGINE IN LOG360

The problem at hand

In today's threat landscape, cyberattacks are becoming more targeted and evasive. From ransomware and insider threats to SQL injection and data exfiltration, these attacks often span multiple devices, events, and logs, making it a challenge to detect them using isolated indicators.

Many organizations struggle to correlate these events in real time due to their reliance on traditional log monitoring systems or reactive alerting mechanisms. As a result, attackers may operate undetected for extended periods.

Security teams need a powerful engine that can analyze multiple log sources simultaneously, understand complex attack chains, delve into advanced forensics and root cause analysis, and generate actionable insights in real time. All this has to be done without overwhelming analysts with noise.

The real-time correlation engine in Log360: Rule-based, instantaneous detection

The real-time correlation engine in ManageEngine Log360 is designed to proactively identify cyberattacks and help you respond to them by analyzing logs and events from across your IT environment using predefined and customizable correlation rules. With over 200 built-in rules and growing, it can instantly detect known attack patterns such as ransomware infections, brute-force logons, lateral movement, privilege abuse, and SQL injection attempts.

Log360 provides the Correlation Rule Library: a curated collection of over 200 in-depth detection rules with detailed descriptions, MITRE ATT&CK® linkages, attack chain scenarios, false positives, and next steps to take.

Security analysts can also build their own rules using an intuitive correlation rule builder featuring advanced filters, over 200 out-of-the-box action events, and custom action events—all without writing a single line of code.

Benefits of the real-time correlation engine

- Real-time threat detection
- Attack surface coverage spanning most network devices
- A custom rule builder for contextual use case detection
- Automated incident response
- Reduced false positives

How the real-time correlation engine works

The real-time correlation engine monitors incoming log events from endpoints, servers, applications, and network devices. It continuously scans these events for defined patterns that match attack behaviors.

Below are a few out-of-the-box correlation rules for detection that are available in Log360:

- Brute-force attacks
- Anomalous user account changes
- Suspicious registry modifications
- SQL injection attacks for web servers and databases
- Suspicious parent and child processes

Custom rules can be created using:

- Predefined or custom granular events across network devices.
- Criteria that can be set based on fields such as the device type or name, IP addresses, Security Account Manager account name, WLAN standard, and globally unique identifier.
- Logical conditions such as equals, contains, starts with, and is constant.
- Sequences of actions.
- Threshold-based filters.
- Time-based chaining of events (e.g., event A to event B to event C within five minutes).

Once a rule condition is met, the system generates an alert within the product. The analyst can link an alert profile to a correlation rule, which will enable them to leverage Log360's automated response workflows. Alert profiles can be used to trigger automated workflows such as Active Directory actions, CSV lookups, killing processes, disabling computers, and other custom workflows.

Real-life use cases handled by Log360

Security analysts leverage Log360's real-time correlation engine for numerous use cases. Here are five use cases that Log360 caters to:

Ransomware detection

User account takeover detection

File integrity threat detection

Web server exploitation detection

Insider threat detection

Below, we will go over the attack chains for these use cases and the built-in rules in Log360 that help detect these threats. Please note that there are numerous ways Log360 can detect these; below, we mention just a single example of each use case.

Ransomware detection

Example of a ransomware attack chain

1. An attacker gains an initial foothold; *wermgr.exe* spawns an unusual child process (e.g., cmd.exe).
2. They escalate via obfuscated PowerShell commands.
3. They use *taskkill.exe* excessively to terminate backup processes.
4. They launch taskhost.exe to encrypt or exfiltrate files under the radar.

Out-of-the-box rules leveraged by Log360 for detection

- *wermgr* Spawning Suspicious Child
- Excessive Usage Of Taskkill
- Suspicious Encoded PowerShell Command Line
- Suspicious parent spawning taskhost

Log360 correlates these discrete events, helping you identify a ransomware storyline, instantly alerting SOC teams, and triggering containment workflows.

User account takeover detection

Example of a user account takeover attack chain

1. An attacker uses brute force to compromise a user account.
2. They execute obfuscated PowerShell commands to stay hidden.
3. They dump credentials using Mimikatz or a similar tool.

Out-of-the-box rules leveraged by Log360 for detection

- Suspicious Encoded PowerShell Command Line
- MimiKatz Detection
- Brute force

Log360 leverages multiple rules within its library to detect lateral movement and unauthorized privileged access, enabling security teams to quickly isolate affected users.

File integrity threat detection

Example of a file integrity threat attack chain

1. An attacker abuses a native process (taskkill) to disable security software.
2. They spawn a child process to modify files in protected directories.
3. They launch background processes (like taskhost) to mask changes.

Out-of-the-box rules leveraged by Log360 for detection

- Excessive Usage Of Taskkill
- wermgr Spawning Suspicious Child
- Suspicious parent spawning taskhost

This is ideal for detecting file tampering, policy bypassing, and log wiping techniques often used before or after data theft. Leverage Log360 for your organization now.

Web server exploitation detection

Example of a web server exploitation attack chain

1. An attacker exploits an SQL injection vulnerability to gain access to the web server.
2. They execute encoded PowerShell commands for persistence.
3. They launch taskhost.exe for data exfiltration.

Out-of-the-box rules leveraged by Log360 for detection

- Suspicious Encoded PowerShell Command Line
- Suspicious parent spawning taskhost
- Repeated SQL injection attempts

Log360 correlates web logs, PowerShell command usage, and system process chains to detect active server compromise.

Insider threat detection

Example of an insider threat (data theft) attack chain

1. A trusted user executes a suspicious PowerShell command to bypass DLP tools.
2. They gain access to sensitive folders.
3. They transfer data to unauthorized locations or removable devices.

Out-of-the-box rules leveraged by Log360 for detection

- Suspicious Encoded PowerShell Command Line
- wermgr Spawning Suspicious Child
- Suspicious file access

Log360 provides real-time insights into anomalous file activity combined with command-line abuse, aiding insider threat detection programs. Log360 also leverages its advanced ML-backed UEBA capabilities to detect malicious insider behavior that deviates from the baseline.

ManageEngine

Log360

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, an analytical Incident Workbench, 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.

Personalized Demo

Download