ManageEngine
Log360

DATASHEET

# SMART THRESHOLD in Log360

## How many alerts are too many?

As a security analyst, have you ever been stuck with the dilemma of setting a threshold value for your alerts? Have you found yourself in a labyrinth, unable to decipher patterns, though you spend hours looking for them? If so, the Smart Threshold capability in Log360 is for you. It's alerting made easy with machine learning (ML)!

# The problem

Configuring an alert is one of the most vital steps in your defense against cyberthreats. If not configured rightly, you could miss out on important threats that cost you your entire business. Research shows that SOCs encounter close to 11,000 alerts daily and engage in redundant triaging processes. What could this mean? Alert fatigue, longer work hours, increased manual efforts, and most importantly, overlooking threats that matter.

Security teams have long used threshold filters to reduce alert overload. A threshold is usually specified by the number of events and the time interval within which they occur. If the threshold is exceeded, a single alert is generated for all these events.

However, it can be difficult to determine the threshold for each event type. Security teams may end up keeping thresholds too high or too low.

- Keeping them too low, you are bombarded with false positives.
- Keeping them too high, you miss out on threats.

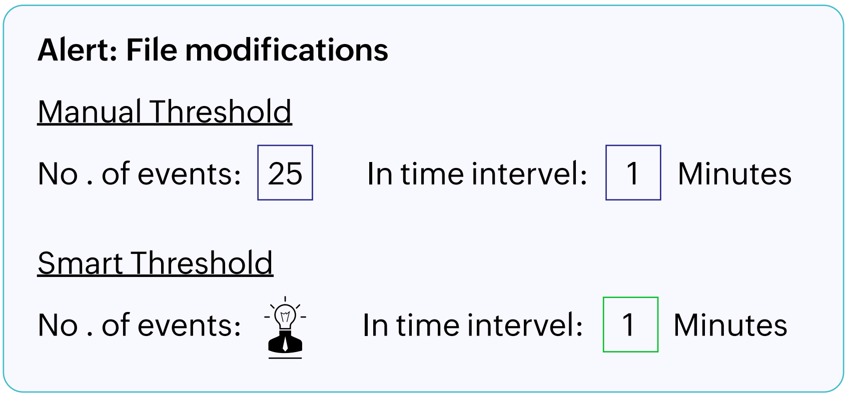
But the good news is, you can now switch to the new Smart Threshold feature in Log360.

# Smart Threshold: ML-led security alerting

Traditional threshold-setting methods often rely on human-defined rules and thresholds, which can be time-consuming, prone to errors, and may not effectively capture the full complexity of the network environment. By utilizing ML, Smart Threshold in Log360 reduces the reliance on human input and manual configuration. The ML model automatically analyzes typical network behavior to derive a threshold value. The threshold also adapts to changes in network behavior over time. As new patterns emerge, thresholds are adjusted accordingly, ensuring that the detection capability remains accurate and precise, even in dynamic and evolving network environments. Smart Threshold helps to minimize human errors that can occur during threshold setting and allows for more efficient detection of security incidents.

# How it works

With the addition of Smart Threshold in Log360, analysts just need to specify the desired time interval while creating alerts. The ML algorithm understands your environment by creating a baseline with the expected number of events for a few hours initially before the actual threat detection begins.



**Alert: File modifications**

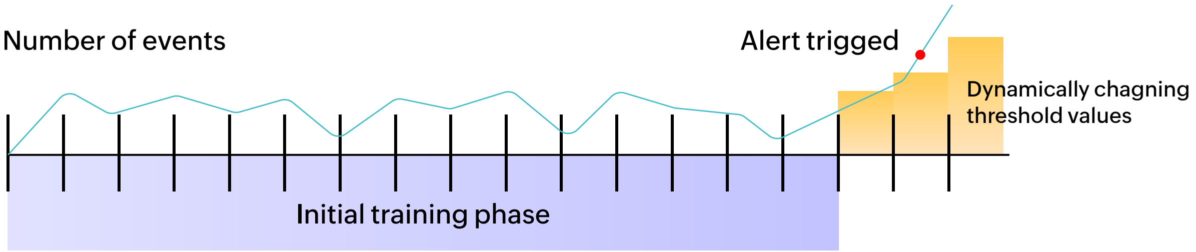
Manual Threshold

No . of events: 25 In time intervel: 1 Minutes

Smart Threshold

No . of events: In time intervel: 1 Minutes

The training period for Smart Threshold is usually 15 times the specified time interval. For instance, the training period is 2.5 hours for a time interval of 10 minutes, meaning the minimum time required for the first alert to be generated is 2.5 hours. The threshold value is dynamically updated subsequently at 10-minute intervals.



**Note:** If any of the following adjustments is made to the Smart Threshold settings: criteria change, device change, change in time range or a switch to manual threshold, then the model will undergo a new training period.

## Benefits of Smart Threshold

Smart Threshold brings greater precision and automation to threat detection in Log360, allowing security teams to focus on real threats and respond effectively to mitigate risks.

- Security analysts need not specify the threshold value for alerts. This saves time and helps them add more alert profiles with confidence for effective threat detection.
- Achieve precise anomaly detection, as the threshold value is constantly learned and updated to reflect changing behaviors.
- Reduce alert overload and alert fatigue for security teams with the reduction in false positives.

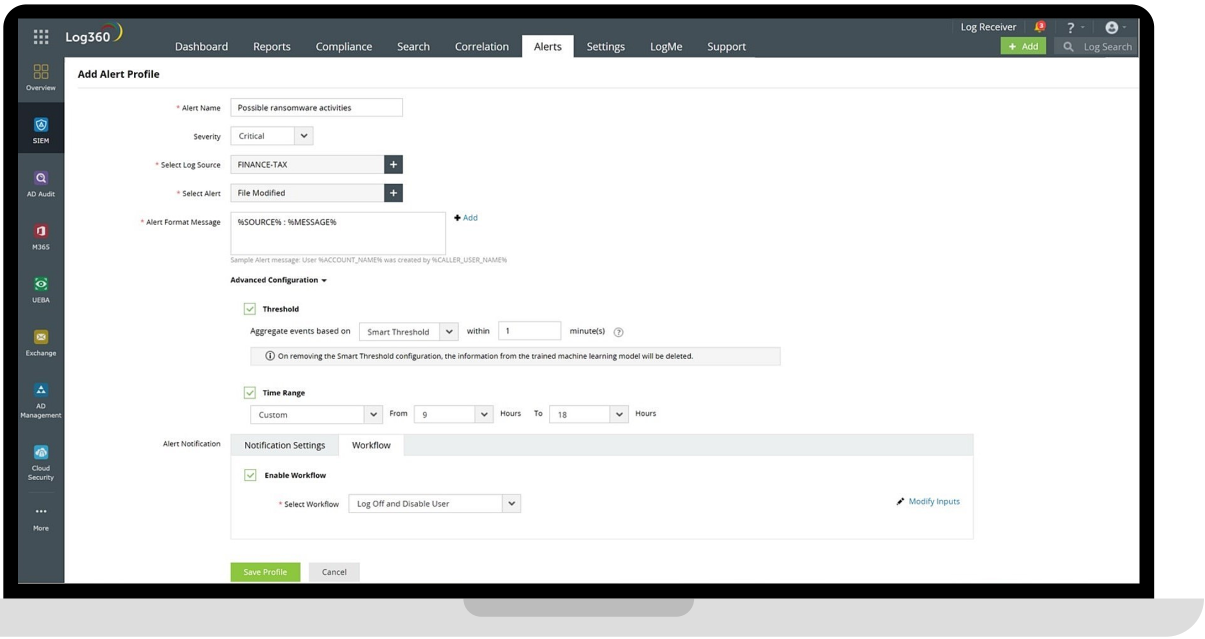
# Use cases

## 1 Ransomware detection

- Ransomware attacks often involve a rapid and widespread encryption or modification of files. But differentiating between legitimate file modifications and malicious modifications can be tricky. The Smart Threshold feature for such attacks can be configured for short intervals, like every one minute.

- After the training phase, 15 minutes in this case, the model generates dynamic threshold values for file modifications every minute. Any sudden spike in the number of file modifications beyond the established baseline are flagged as potential ransomware activity, triggering an alert for immediate investigation.

The image below shows the configuration of an Alert Profile for detecting possible ransomware activity.



Add Alert Profile

* Alert Name: Possible ransomware activities

Severity: Critical

* Select Log Source: FINANCE-TAX

* Select Alert: File Modified

* Alert Format Message: %SOURCE% : %MESSAGE%

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Advanced Configuration

☑ Threshold

Aggregate events based on Smart Threshold within 1 minute(s)

ⓘ On removing the Smart Threshold configuration, the information from the trained machine learning model will be deleted.

☑ Time Range

Custom From 9 Hours To 18 Hours

Alert Notification: Notification Settings | Workflow

☑ Enable Workflow

* Select Workflow: Log Off and Disable User

Modify Inputs

Save Profile | Cancel

## 2 DDoS attack detection

- DDoS attacks are characterized by a high volume of denied connections to network services. The Smart Threshold feature for such attacks can be configured with a suitable interval, such as two minutes.

- During the training period, which is 30 minutes in this case, the system learns the expected rate of denied connections every two minutes and establishes a baseline.

- After the training phase, the system generates dynamic thresholds for denied connections every two minutes. Any unusual surge in denied connections exceeding the established threshold could indicate an ongoing DDoS attack, triggering alerts for investigation and mitigation.

## 3 System activity and application crashes

- Anomalies related to system activity, such as application crashes, can impact system stability and security. Smart Threshold can help identify such incidents.

- A suitable interval for the threshold can be configured, such as every 30 minutes. During the initial 7.5 hour training phase, the system learns about the expected number of application crashes.

- After the training phase, the system generates dynamic thresholds for application crashes every 30 minutes. If the rate of application crashes or unusual activity exceeds the established thresholds, the system generates alerts to investigate potential security breaches or system issues.

Other use cases for Smart Threshold include:

- **Brute-force attacks:** A high count of failed user logon events.
- **Malware activities:** Excessive registry modification events and service started events.
- **Lateral movement:** High number of accesses to network shares.
- **C2 attack:** Unexpected volume of outbound connections.

In all these use cases, Log360, with its Smart Threshold feature, enables you to adapt to changing circumstances and evolving threat landscapes by dynamically adjusting thresholds based on historical data. This proactive approach enhances Log360's ability to detect anomalies and respond to potential security incidents in real time.