ManageEngine
Log360

Precision in action:

# Leveraging smart thresholds for accurate detection

www.manageengine.com/log-management/

# Introduction

*Security information and event management (SIEM) solutions are central to the modern cybersecurity landscape, continuously monitoring vast amounts of data to identify and respond to potential threats.*

These threats can come from various sources, including suspicious login attempts, malware activity, or unauthorized data access. By analyzing security logs and events, SIEM solutions generate alerts notifying security teams of potential issues. These alerts work based on set thresholds.

Thresholds are predefined limits that trigger alerts or actions when certain conditions are met. While static thresholds have been a common approach, they come with several challenges that can impact the efficacy of threat detection.

Static thresholds, characterized by preset values, are like predetermined molds that do not conform to the changing shapes of modern cyber risks. This leads to false positives and negatives. These fixed benchmarks, established based on historical data or assumptions about normal network behavior, often fall short in accommodating the complexity of diverse IT environments that include a wide range of applications, devices, and user behaviors.

Businesses often experience seasonal variations in their network traffic and user behavior. Static thresholds struggle to accommodate such fluctuations, potentially causing alert fatigue or overlooking abnormal patterns during peak times.

To address these challenges, smart thresholds emerge as a solution that brings a dynamic and context-aware approach to SIEM solutions.

# The concept of smart thresholds

Smart thresholds are dynamic parameters that leverage contextual information and real-time data to continuously reassess and readjust their values. Unlike static thresholds, which are fixed values set based on predefined standards, smart thresholds have the capability to adjust dynamically in response to changes in the IT environment.

This adaptability allows organizations to account for fluctuations in normal network activity, user behavior, and system performance. It helps distinguish between normal and potentially malicious activities, reducing the likelihood of false positives and enhancing the accuracy of threat detection.

# How does it work?

**a. Baseline establishment:**

A SIEM solution establishes a baseline of normal behavior for various entities within the environment, such as users, devices, and applications.

The smart threshold feature automatically determines the number of events that will be ideal for reducing false positive triggers by analyzing historical data and understanding the typical patterns of activity using machine learning (ML) algorithms.

**b. Continuous monitoring and adjustment:**

Once a baseline is established, the network environment is continuously monitored for deviations from the established baseline. Based on the ongoing analysis, the SIEM solution dynamically adjusts the thresholds for different parameters.

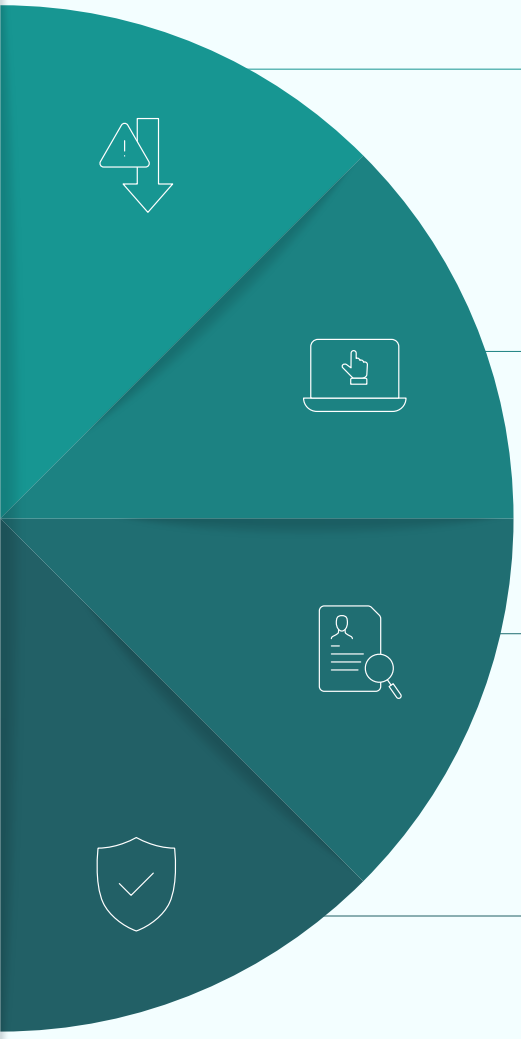
For example, if there is a sudden spike in login attempts but it aligns with the normal pattern of behavior during a specific time of day, the solution may adjust the threshold to avoid unnecessary alerts.

**c. Alert generation:**

When the observed activities exceed the dynamically adjusted thresholds, the SIEM solution generates alerts and triggers automated workflows.

These alerts are indicative of potentially malicious activities, which may escalate into attacks if immediate attention is not given.

# Benefits of smart thresholds



### Reduced alert noise:

Dynamically adjusting thresholds helps to screen known patterns of benign behavior, thereby reducing alert fatigue. This approach avoids unnecessary alerts and helps security teams focus on the important issues.

### Immediate action:

Since the security team is now freed from the burden of giving time and attention to false positives and low priority, non-threat events, they can now invest their time and energy into quickly addressing critical threats.

### Low manual intervention:

The alert threshold is periodically revised based on the log source and alert criteria, which otherwise would have been a huge task for the security team to do manually.

### Adaptability:

Smart thresholds ensure ongoing relevance, accommodating changes in the network and user behavior by using statistical ML models. By doing so, they ensure that security measures remain effective and relevant in the face of organizational growth.

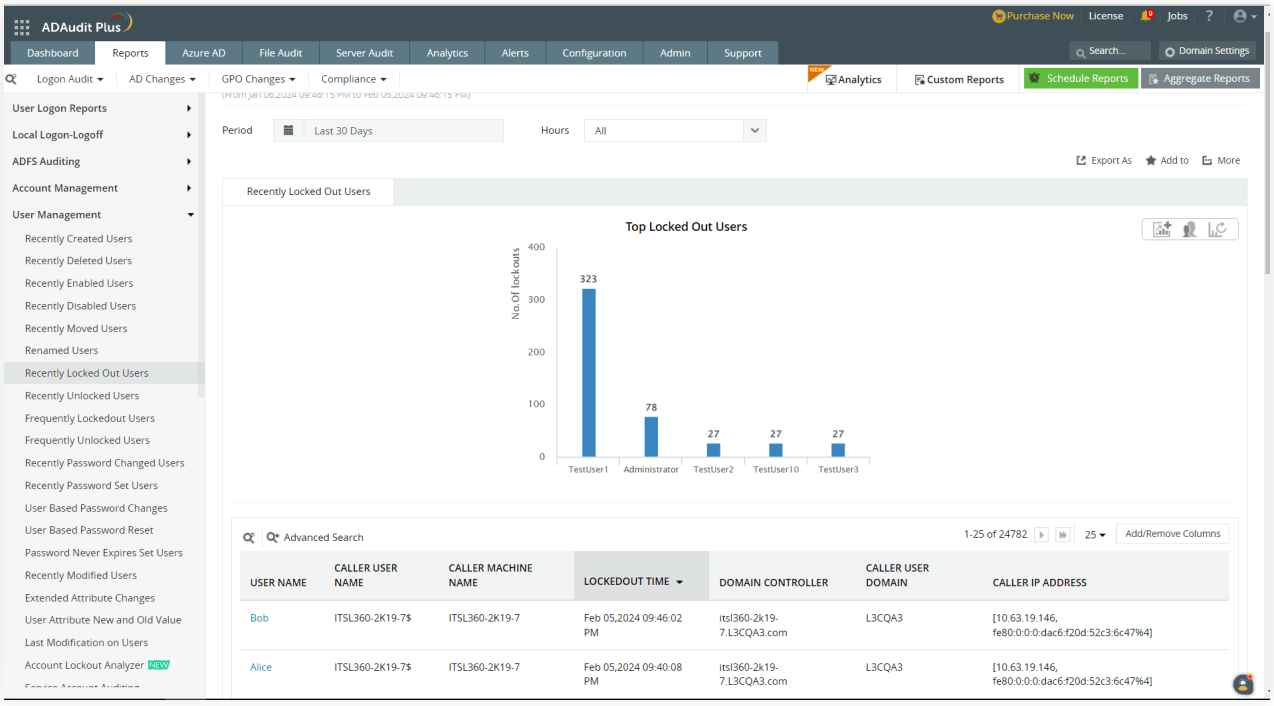
# Log360's smart thresholds

Let's delve into how the smart threshold feature operates in real-time scenarios. Say a large organization's security team frequently receives alerts about account lockouts in their Active Directory environment. Investigating each lockout is time-consuming, and many of these may simply occur due to users entering incorrect passwords.

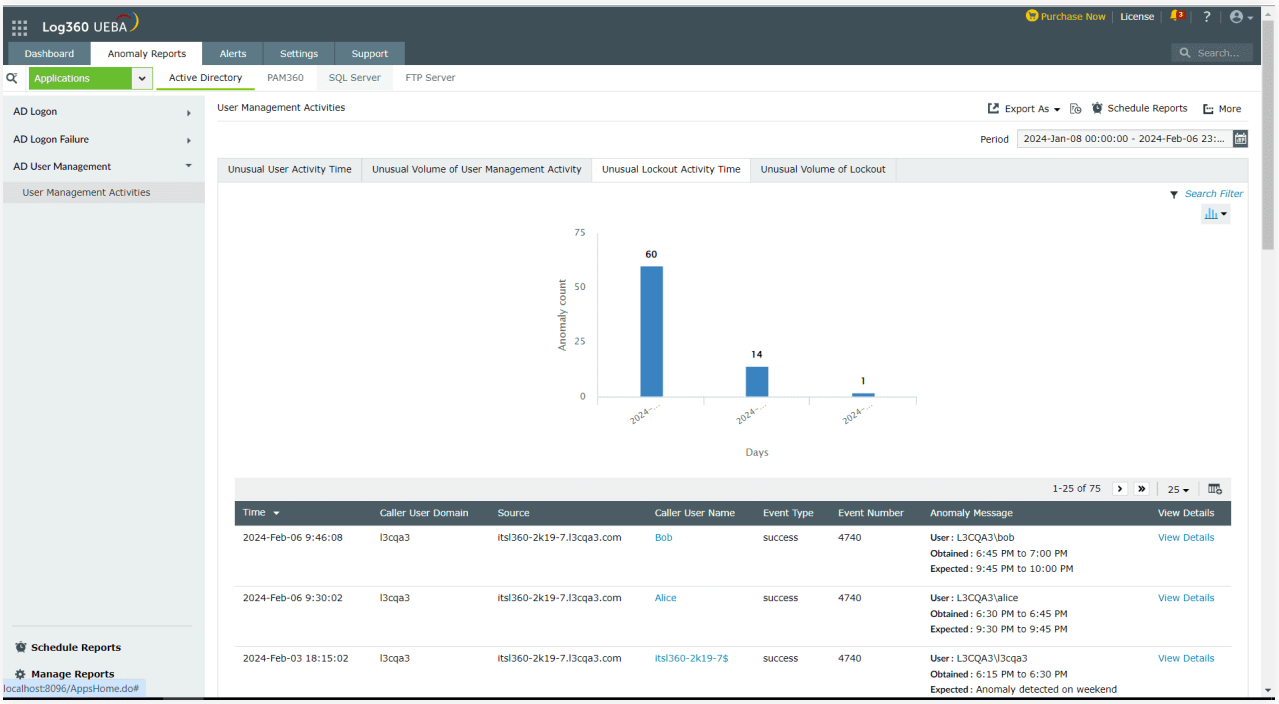
Consider a scenario where employees regularly update their passwords during a specific time of the year. As expected, this leads to an increase in instances of wrong password entries and, subsequently, more account lockouts. Without a smart threshold feature, a SIEM solution could flood the security team with numerous alerts during this period, potentially burying critical alerts indicating actual attacks.

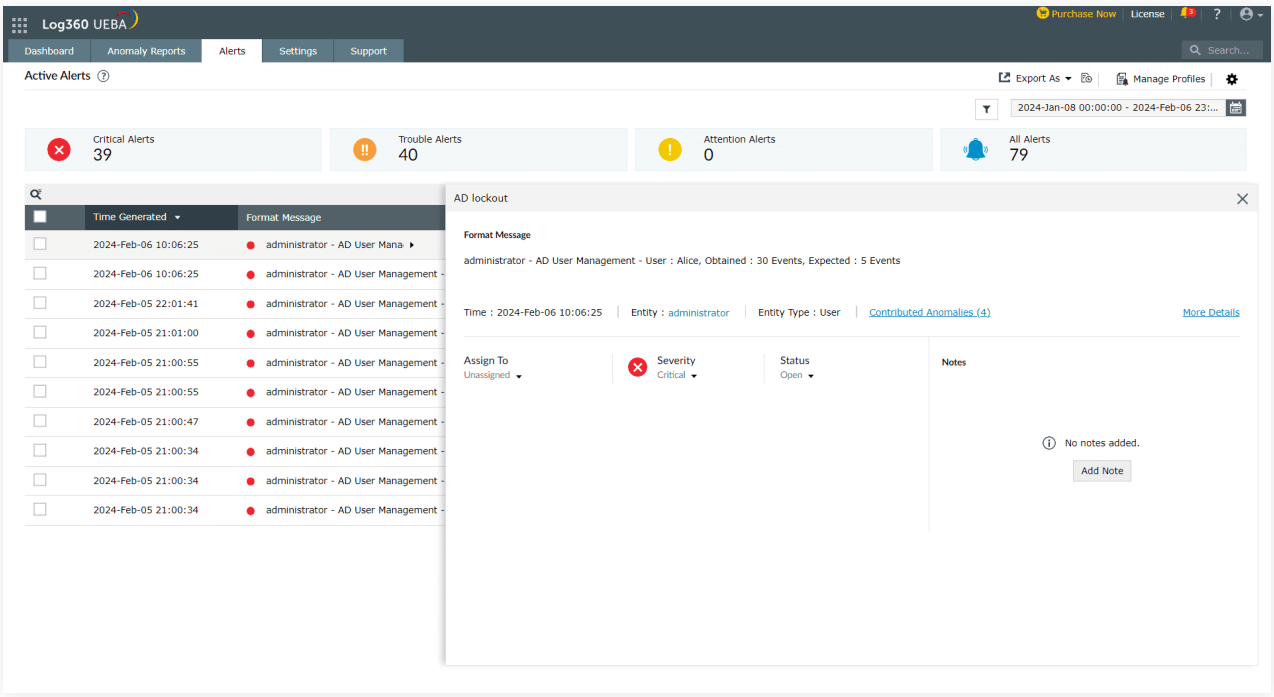
Log360's smart thresholds, coupled with its UEBA module, provide dual-layered threat detection, effectively filtering out non-threatening alerts. While UEBA detects anomalies based on patterns, the smart threshold feature focuses on count-based anomaly detection.
To understand this context better, consider the following use case.

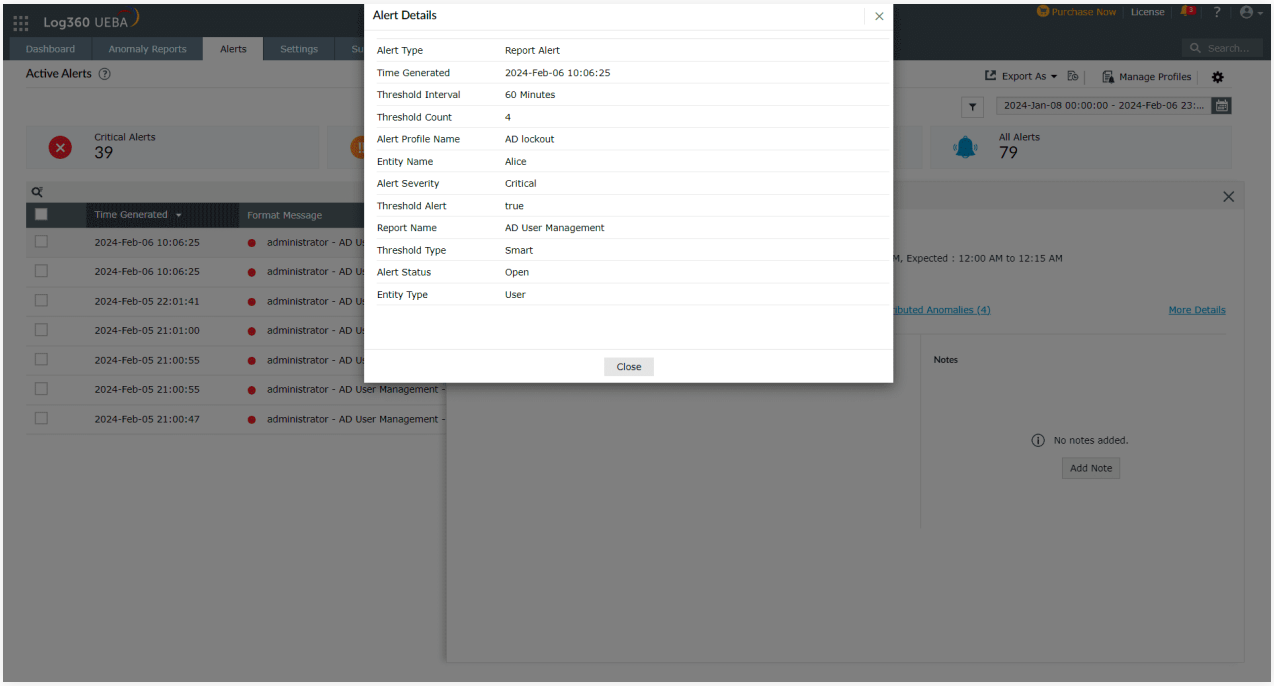
In this use case, Log360 UEBA draws insights from the ADAudit Plus account lockout report. Using these insights, Log360's UEBA offers predefined, time-based anomaly reports. Alerts are triggered based on the smart threshold set for this particular report. When the frequency of time-based anomalies exceeds this threshold, an alert is issued.



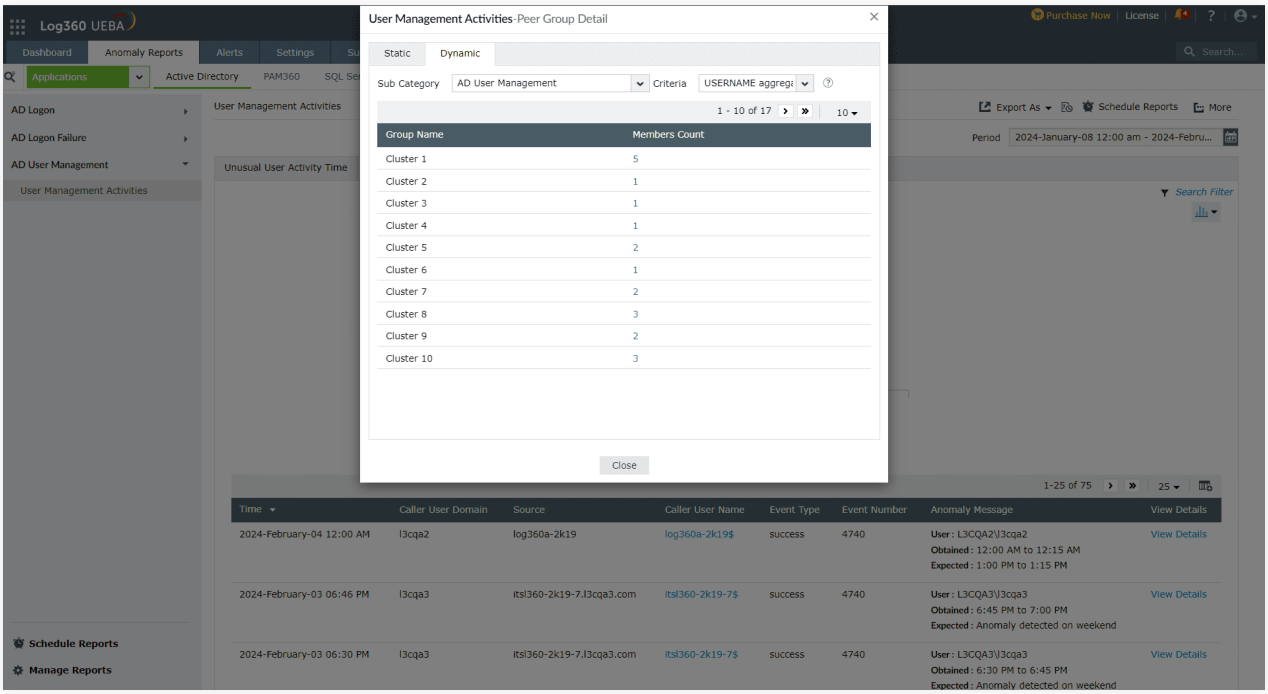
Let's take the scenario of two users, Alice and Bob, encountering account lockouts due to password entry errors. Upon surpassing the set threshold, an alert is promptly triggered for Alice, as she is the first within the organization to reach this threshold. Initially set at 4, the smart threshold is now adjusted to 5 in response to this incident, as reflected in the alert details.

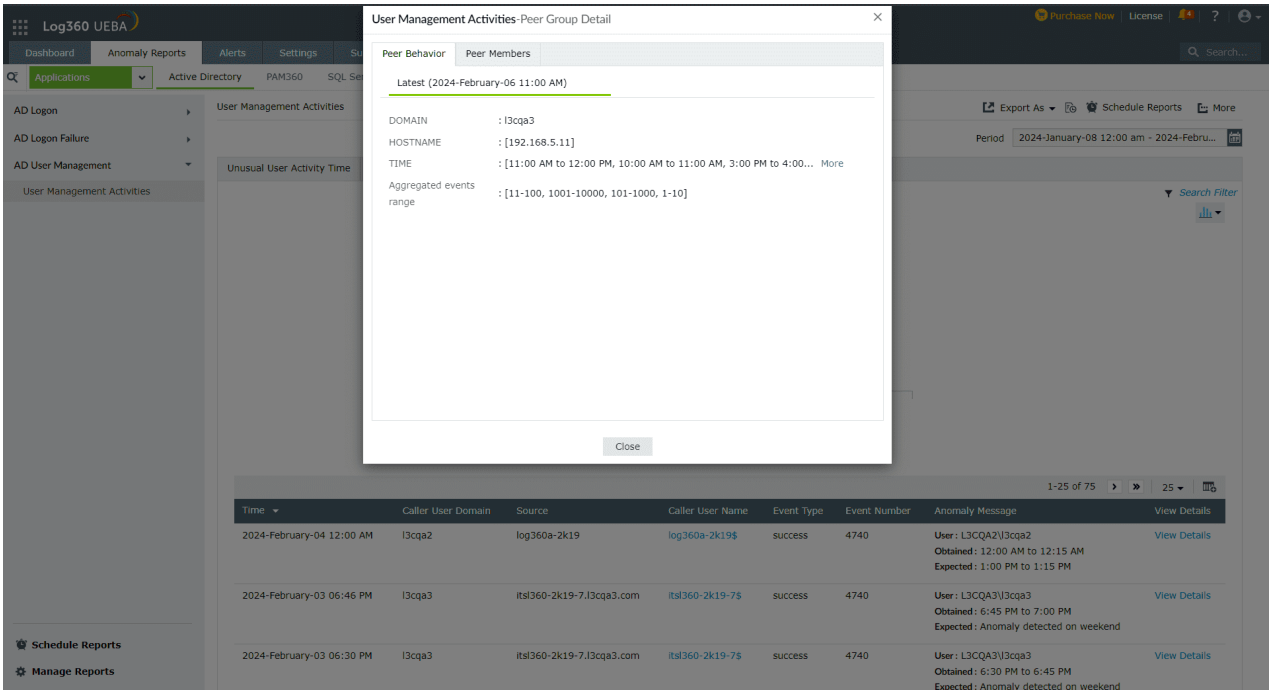


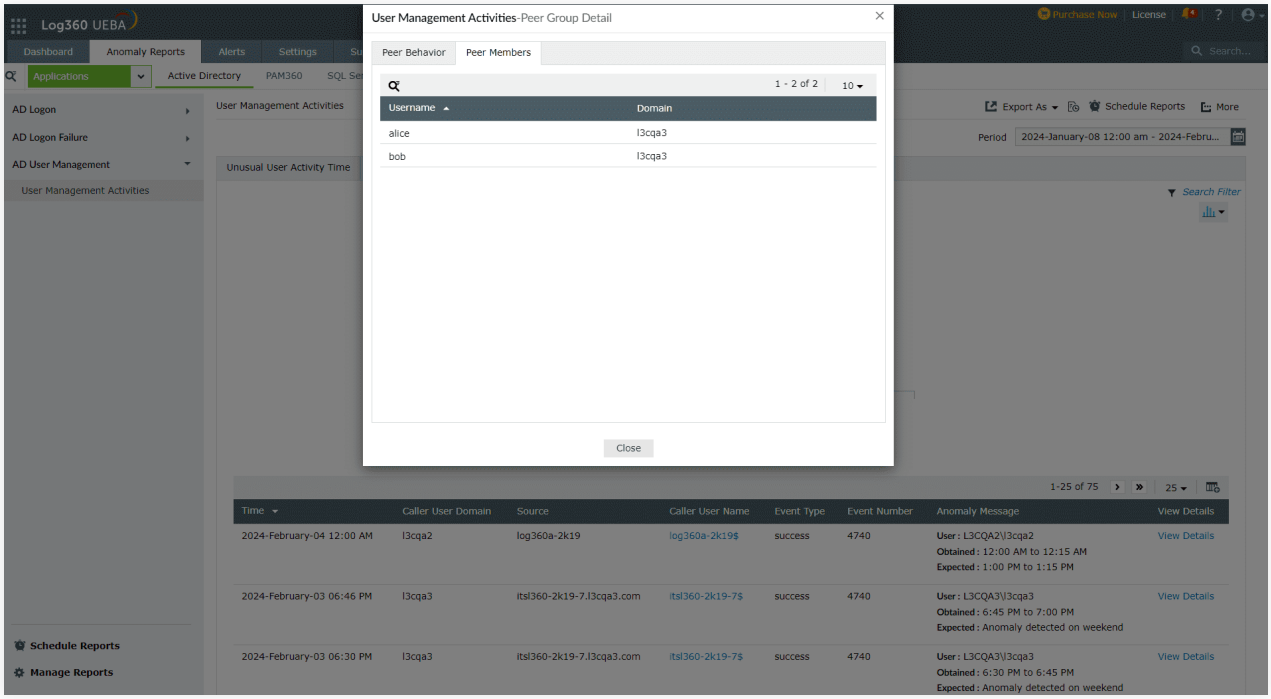






Utilizing dynamic peer grouping, both Alice and Bob are clustered together due to their similar activities. Consequently, Bob's risk score remains unaffected since he is associated with Alice in the same cluster. This ensures that an alert is not triggered for Bob.




Log360 UEBA
User Management Activities-Peer Group Detail
Peer Behavior
Peer Members
Latest (2024-February-06 11:00 AM)
DOMAIN : l3cqa3
HOSTNAME : [192.168.5.11]
TIME : [11:00 AM to 12:00 PM, 10:00 AM to 11:00 AM, 3:00 PM to 4:00... More
Aggregated events range : [11-100, 1001-10000, 101-1000, 1-10]
Close
Dashboard
Anomaly Reports
Alerts
Settings
Applications
Active Directory
PAM360
AD Logon
AD Logon Failure
AD User Management
User Management Activities
Unusual User Activity Time
Export As
Schedule Reports
More
Search Filter
Schedule Reports
Manage Reports
Time
Caller User Domain
Source
Caller User Name
Event Type
Event Number
Anomaly Message
View Details
2024-February-04 12:00 AM
2024-February-03 06:46 PM
2024-February-03 06:30 PM


Log360 UEBA
User Management Activities-Peer Group Detail
Peer Behavior
Peer Members
Username
Domain
alice
bob
l3cqa3
Close
Dashboard
Anomaly Reports
Alerts
Settings
Applications
Active Directory
PAM360
AD Logon
AD Logon Failure
AD User Management
User Management Activities
Unusual User Activity Time
Export As
Schedule Reports
More
Search Filter
Schedule Reports
Manage Reports
Time
Caller User Domain
Source
Caller User Name
Event Type
Event Number
Anomaly Message
View Details
2024-February-04 12:00 AM
2024-February-03 06:46 PM
2024-February-03 06:30 PM

In this case, when there is a surge in account lockouts, Log360's smart threshold feature considers the broader context of account lockouts across the network and adjusts the count-based threshold accordingly. Simultaneously, UEBA's dynamic peer grouping feature organizes users based on their behaviors, contextualizing the event within the cluster's activity. Given the high frequency of account lockouts during the password update period, the risk score for such events is appropriately regulated.

Together, these actions ensure that alerts are not needlessly triggered for benign events, alleviating the burden on the security team. This approach increases the likelihood of the security team promptly addressing meaningful alerts that may indicate potential attacks, thereby enhancing overall security responsiveness and reducing the risk of overlooking critical security threats.

In conclusion, smart thresholds provide effective defense against evolving threats while minimizing manual intervention and optimizing resource allocation. Embracing the feature is crucial for organizations aiming to stay ahead in the dynamic cybersecurity landscape.

## Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus

Exchange Reporter Plus | M365 Manager Plus

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.

$ Get Quote  Download