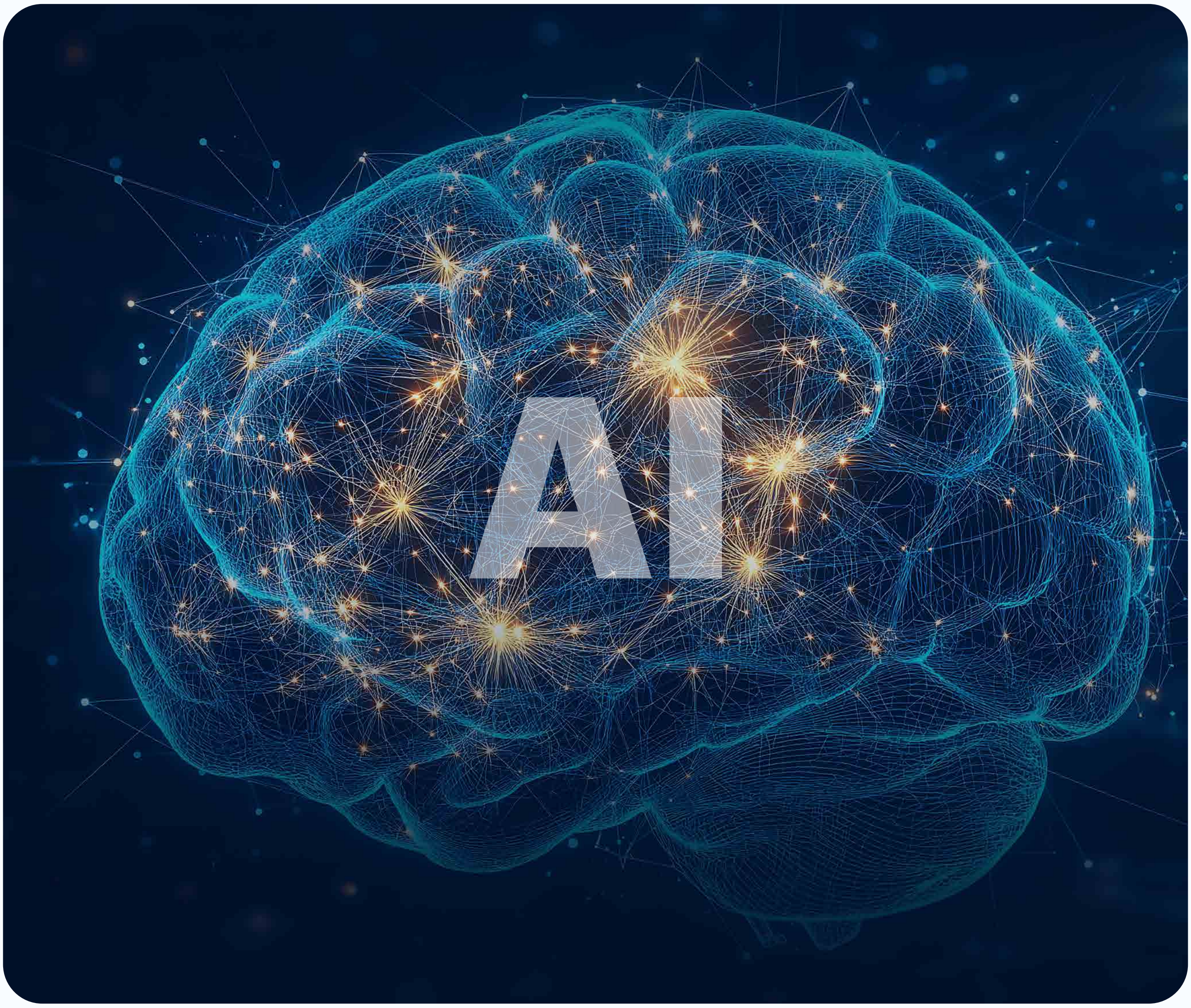
ManageEngine
Log360

DATASHEET

Zia Insights AI-powered security analytics in Log360



Overview

Security analysts today face an overwhelming volume of alerts and logs. Time spent manually investigating incidents can delay response and increases risk exposure. Zia Insights bridges this gap with contextual, AI-generated summaries across logs, alerts, and incidents, delivering instant clarity so teams can act faster and with confidence.

Designed for rapid contextualization of security data, Zia delivers actionable insights that transform how analysts investigate and respond to threats. Built on the robust Zia AI platform, trusted across over 100 Zoho apps, and powered by Azure OpenAI with a bring-your-own-key model, Zia Insights is tailored for enterprise-level intelligence and security analytics.

Note: This feature is currently available only in the cloud version of Log360.

Benefits of Zia Insights

Accelerated threat investigation

Zia analyzes log data and summarizes security incidents with root causes, MITRE mappings, and involved entities. Analysts can go from seeing alerts to understanding the cause in seconds, not hours.

Faster alert triage

With high volumes of false positives, SOCs struggle to prioritize real threats. Zia helps by categorizing alerts, summarizing the threat context, and highlighting user risk scores and attack vectors.

Proactive insider threat detection

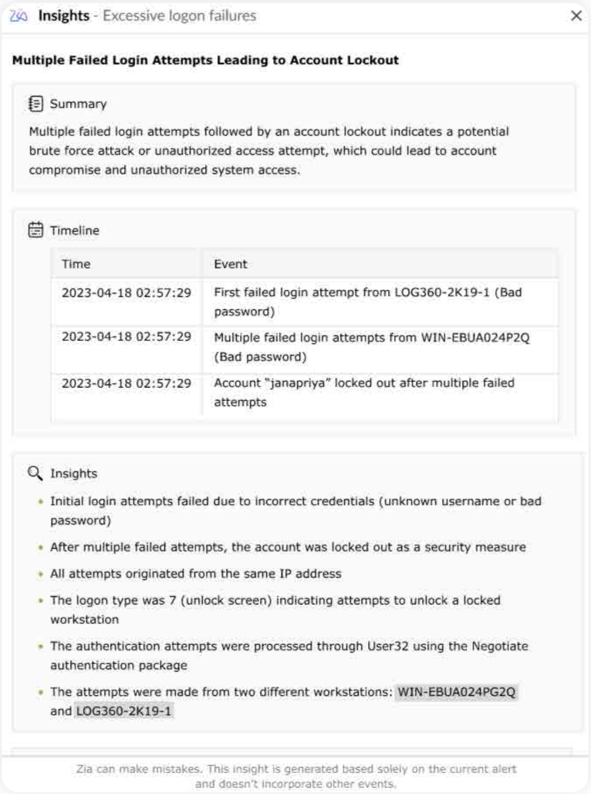
By mapping unusual user behavior to known attack techniques, Zia flags insider threats and risky access attempts with context-aware insights, helping teams take early action.

Crash and error resolution

When systems generate error or crash logs, Zia categorizes them and provides troubleshooting suggestions, helping IT teams restore services and reduce downtime.

Incident reconstruction

Zia generates visual timelines that stitch together logs, alerts, and events, allowing analysts to replay the sequence and understand the full impact and path of an incident.



Multiple Failed Login Attempts Leading to Account Lockout

Summary

Multiple failed login attempts followed by an account lockout indicates a potential brute force attack or unauthorized access attempt, which could lead to account compromise and unauthorized system access.

Timeline

Time	Event
2023-04-18 02:57:29	First failed login attempt from LOG360-2K19-1 (Bad password)
2023-04-18 02:57:29	Multiple failed login attempts from WIN-EBUA024P2Q (Bad password)
2023-04-18 02:57:29	Account "janapriya" locked out after multiple failed attempts

Insights

- Initial login attempts failed due to incorrect credentials (unknown username or bad password)
- After multiple failed attempts, the account was locked out as a security measure
- All attempts originated from the same IP address
- The logon type was 7 (unlock screen) indicating attempts to unlock a locked workstation
- The authentication attempts were processed through User32 using the Negotiate authentication package
- The attempts were made from two different workstations: WIN-EBUA024PG2Q and LOG360-2K19-1

Zia can make mistakes. This insight is generated based solely on the current alert and doesn't incorporate other events.

Highlights of Log360's AI-driven security analytics

Capabilities	How it helps
Contextual summaries	Instantly summarizes logs, events, alerts, and incidents for quick understanding and triage
Automated categorization	Classifies logs into error, audit, and security logs for streamlined analysis
Threat modeling framework mapping	Map attack scenarios to relevant MITRE ATT&CK® tactics and techniques for clear threat context
Timelines	Generates visual timelines for correlated events, alerts, and incidents, aiding root-cause and sequence analysis
Actor and entity attribution	Insights highlights users, systems, and entities involved for faster investigation
Actionable guidance	Provides troubleshooting steps for error logs and potential mitigation steps for threats and attacks

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 on the cloud-version of Log360, please visit
www.manageengine.com/cloud-siem/

$ Get Quote   ⤓ Download